ProSafe XSM7224S Managed Stackable Switch CLI Manual, Software Version 9.0

NETGEAR, Inc.
350 Plumeria Dr.
San Jose, CA 95124 USA

202-10770-01
November 2010

Trademarks

NETGEAR and the NETGEAR logo are registered trademarks, and ProSafe is a trademark of NETGEAR, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders. Portions of this document are copyright Intoto, Inc.

November 2010

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

EN 55 022 Declaration of Conformance

This is to certify that the ProSafe XSM7224S Managed Stackable Switch is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Certificate of the Manufacturer/Importer

It is hereby certified that the ProSafe XSM7224S Managed Stackable Switch has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß dasProSafe XSM7224S Managed Stackable Switch gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Product and Publication Details

Model Number:	XSM7224S
Publication Date:	November 2010
Product Family:	managed switch
Product Name:	ProSafe XSM7224S Managed Stackable Switch
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10770-01
Publication Version Number	1.0

Contents

Chapter 5
Quality of Service (QoS) Commands

Chapter 6
Utility Commands

Chapter 7
Management Commands

About This Manual

This document describes command-line interface (CLI) commands you use to view and configure XSM7224S software. You can access the CLI by using a direct connection to the serial port or by using telnet or SSH over a remote network connection.

➡	**Note:** This document contains both standalone and stacking commands.

Audience

This document is for system administrators who configure and operate systems using XSM7224S software. It provides an understanding of the configuration options of the software.

Software engineers who integrate software into their hardware platform can also benefit from a description of the configuration options.

This document assumes that the reader has an understanding of the software base and has read the appropriate specification for the relevant networking device platform. It also assumes that the reader has a basic knowledge of Ethernet and networking concepts.

Refer to the release notes for the application-level code. The release notes detail the platform-specific functionality of the Switching, Routing, SNMP, Configuration, Management, and other packages. The suite of features the packages support is not available on all the platforms to which software has been ported.

About the Software

The software has two purposes:

- Assist attached hardware in switching frames, based on Layer 2, 3, or 4 information contained in the frames.
- Provide a complete device management portfolio to the network administrator.

Scope

The software encompasses both hardware and software support. The software is partitioned to run in the following processors:

- CPU – This code runs the networking device management portfolio and controls the overall networking device hardware. It also assists in frame forwarding, as needed and specified. This code is designed to run on multiple platforms with minimal changes from platform to platform.
- Networking device processor – This code does the majority of the packet switching, usually at wire speed. This code is platform dependent, and substantial changes might exist across products.

Product Concept

Fast Ethernet and Gigabit Ethernet switching continues to evolve from high-end backbone applications to desktop switching applications. The price of the technology continues to decline, while performance and feature sets continue to improve. Devices that are capable of switching Layers 2, 3, and 4 are increasingly in demand. The software provides a flexible solution to these ever-increasing needs.

The exact functionality provided by each networking device on which the software base runs varies depending upon the platform and requirements of the FASTPATH software.

The software includes a set of comprehensive management functions for managing both the software and the network. You can manage the software by using one of the following three methods:

- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)
- Web-based

Each of the management methods enables you to configure, manage, and control the software locally or remotely using in-band or out-of-band mechanisms. Management is standards-based, with configuration parameters and a private MIB providing control for functions not completely specified in the MIBs.

Conventions, Formats, and Scope

The conventions, formats, and scope of this manual are described in the following paragraphs:

- **Typographical Conventions**. This manual uses the following typographical conventions:

Italic	Emphasis, books, CDs, file and server names, extensions
Bold	User input, IP addresses, GUI screen text
`Fixed`	Command prompt, CLI text, code
italic	URL links

- **Formats**. This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.

Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

- **Scope**. This manual is written for the XSM7224S.

Product Version	ProSafe XSM7224S Managed Stackable Switch
Manual Publication Date	November 2010

Note: Product updates are available on the NETGEAR, Inc. website at *http://kbserver.netgear.com*

How to Print This Manual

To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

Revision History

Part Number	Version Number	Date	Description
202-10770-01	1.0	November 2010	Product update: New firmware and new user Interface

Chapter 1
Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

This chapter describes the CLI syntax, conventions, and modes. It contains the following sections:

Command Syntax

A command is one or more words that might be followed by one or more parameters. Parameters can be required or optional values.

Some commands, such as **`show network`** or **`clear vlan,`** do not require parameters. Other commands, such as **`network parms`**, require that you supply a value after the command. You must type the parameter values in a specific order, and optional parameters follow required parameters. The following example describes the **`network parms`** command syntax:

Format **`network parms`** *`<ipaddr> <netmask> [gateway]`*

- **`network parms`** is the command name.
- *`<ipaddr>`* and *`<netmask>`* are parameters and represent required values that you must enter after you type the command keywords.
- *`[gateway]`* is an optional parameter, so you are not required to enter a value in place of the parameter.

The *CLI Command Reference* lists each command by the command name and provides a brief description of the command. Each command reference also contains the following information:

- Format shows the command keywords and the required and optional parameters.
- Mode identifies the command mode you must be in to access the command.
- Default shows the default value, if any, of a configurable setting on the device.

The **`show`** commands also contain a description of the information that the command shows.

Command Conventions

In this document, the command name is in **`bold`** font. Parameters are in *`italic font`*. You must replace the parameter name with an appropriate value, which might be a name or number. Parameters are order dependent.

The parameters for a command might include mandatory values, optional values, or keyword choices. Table 1 describes the conventions this document uses to distinguish between value types.

Table 1. Parameter Conventions

Symbol	Example	Description
<> angle brackets	`<value>`	Indicates that you must enter a value in place of the brackets and text inside them.
[] square brackets	`[value]`	Indicates an optional parameter that you can enter in place of the brackets and text inside them.
{} curly braces	`{choice1 | choice2}`	Indicates that you must select a parameter from the list of choices.
| Vertical bars	`choice1 | choice2`	Separates the mutually exclusive choices.
[{}] Braces within square brackets	`[{choice1 | choice2}]`	Indicates a choice within an optional element.

Common Parameter Values

Parameter values might be names (strings) or numbers.To use spaces as part of a name parameter, enclose the name value in double quotes. For example, the expression “System Name with Spaces” forces the system to accept the spaces. Empty strings (““) are not valid user-defined strings. Table 2 describes common parameter values and value formatting.

Table 2. Parameter Descriptions

Parameter	Description

ipaddr	This parameter is a valid IP address. You can enter the IP address in the following formats:
	`a (32 bits)`
	`a.b (8.24 bits)`
	`a.b.c (8.8.16 bits)`
	`a.b.c.d (8.8.8.8)`
	In addition to these formats, the CLI accepts decimal, hexadecimal and octal formats through the following input formats (where *n* is any valid hexadecimal, octal or decimal number):
	`0xn (CLI assumes hexadecimal format)`
	`0n (CLI assumes octal format with leading zeros)`
	`n (CLI assumes decimal format)`

ipv6-address	`FE80:0000:0000:0000:020F:24FF:FEBF:DBCB, or`
	`FE80:0:0:0:20F:24FF:FEBF:DBCB, or`
	`FE80::20F24FF:FEBF:DBCB, or`
	`FE80:0:0:0:20F:24FF:128:141:49:32`
	For additional information, refer to RFC 3513.

Interface or unit/slot/port	Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1.
Logical Interface	Represents a logical slot and port number. This is applicable in the case of a port-channel (LAG). You can use the logical unit/slot/port to configure the port-channel.
Character strings	Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

Unit/Slot/Port Naming Convention

Managed switch software references physical entities such as cards and ports by using a unit/slot/port naming convention. The software also uses this convention to identify certain logical entities, such as Port-Channel interfaces.

The slot number has two uses. In the case of physical ports, it identifies the card containing the ports. In the case of logical and CPU ports it also identifies the type of interface or port.

Table 3. Type of Slots

Slot Type	Description
Physical slot numbers	Physical slot numbers begin with zero, and are allocated up to the maximum number of physical slots.
Logical slot numbers	Logical slots immediately follow physical slots and identify port-channel (LAG) or router interfaces.
CPU slot numbers	The CPU slots immediately follow the logical slots.

The port identifies the specific physical port or logical interface being managed on a given slot.

Table 4. Type of Ports

Port Type	Description
Physical Ports	The physical ports for each slot are numbered sequentially starting from zero.
Logical Interfaces	Port-channel or Link Aggregation Group (LAG) interfaces are logical interfaces that are only used for bridging functions. VLAN routing interfaces are only used for routing functions. Loopback interfaces are logical interfaces that are always up. Tunnel interfaces are logical point-to-point links that carry encapsulated packets.
CPU ports	CPU ports are handled by the driver as one or more physical entities located on physical slots.

Note: In the CLI, loopback and tunnel interfaces do not use the unit/slot/port format. To specify a loopback interface, you use the loopback ID. To specify a tunnel interface, you use the tunnel ID.

Using the “No” Form of a Command

The **no** keyword is a specific form of an existing command and does not represent a new or distinct command. Almost every configuration command has a **no** form. In general, use the **no** form to reverse the action of a command or reset a value back to the default. For example, the **no**

`shutdown` configuration command reverses the shutdown of an interface. Use the command without the keyword **`no`** to re-enable a disabled feature or to enable a feature that is disabled by default. Only the configuration commands are available in the **`no`** form.

Managed Switch Modules

Managed switch software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The commands and command modes available on your switch depend on the installed modules. Additionally, for some **`show`** commands, the output fields might change based on the modules included in the software.

The software suite includes the following modules:

- Switching (Layer 2)
- Quality of Service
- Management (CLI, Web UI, and SNMP)
- IPv6 Management—Allows management of the device through an IPv6 through an IPv6 address without requiring the IPv6 Routing package in the system. The management address can be associated with the network port (front-panel switch ports), a routine interface (port or VLAN) and the Service port.
- Stacking

Not all modules are available for all platforms or software releases.

Command Modes

The CLI groups commands into modes according to the command function. Each of the command modes supports specific software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

The command prompt changes in each command mode to help you identify the current mode. Table 5 describes the command modes and the prompts visible in that mode.

Note: The command modes available on your switch depend on the software modules that are installed. For example, a switch that does not support BGPv4 does not have the Router BGPv4 Command Mode.

Table 5. CLI Command Modes

Command Mode	Prompt	Mode Description
User EXEC	`Switch>`	Contains a limited set of commands to view basic system information.
Privileged EXEC	`Switch#`	Allows you to issue any **EXEC** command, enter the VLAN mode, or enter the Global Configuration mode.
Global Config	`Switch (Config)#`	Groups general setup commands and permits you to make modifications to the running configuration.
VLAN Config	`Switch (Vlan)#`	Groups all the VLAN commands.
Interface Config	Switch (Interface <unit/slot/port>)# Switch (Interface Loopback <id>)# Switch (Interface Tunnel <id>)#	Manages the operation of an interface and provides access to the router interface configuration commands. Use this mode to set up a physical port for a specific logical connection operation.
Line Config	Switch (line)#	Contains commands to configure outbound telnet settings and console interface settings.
Policy Map Config	Switch (Config-policy-map)#	Contains the QoS Policy-Map configuration commands.
Policy Class Config	Switch (Config-policy-class-map)#	Consists of class creation, deletion, and matching commands. The class match commands specify Layer 2, Layer 3, and general match criteria.
Class Map Config	Switch (Config-class-map)#	Contains the QoS class map configuration commands for IPv4.
Ipv6_Class-Map Config	Switch (Config-class-map)#	Contains the QoS class map configuration commands for IPv6.
Router OSPF Config	Switch (Config-router)#	Contains the OSPF configuration commands.
Router OSPFv3 Config	Switch (Config rtr)#	Contains the OSPFv3 configuration commands.
Router RIP Config	Switch (Config-router)#	Contains the RIP configuration commands.
Router BGP Config	Switch (Config-router)#	Contains the BGP4 configuration commands.
MAC Access-list Config	Switch (Config-mac-access-list)#	Allows you to create a MAC Access-List and to enter the mode containing MAC Access-List configuration commands.

Table 5. CLI Command Modes (continued)

Command Mode	Prompt	Mode Description
TACACS Config	Switch (Tacacs)#	Contains commands to configure properties for the TACACS servers.
DHCP Pool Config	Switch (Config dhcp-pool)#	Contains the DHCP server IP address pool configuration commands.
DHCPv6 Pool Config	Switch (Config dhcp6-pool)#	Contains the DHCPv6 server IPv6 address pool configuration commands.
Stack Global Config Mode	Switch (Config stack)#	Allows you to access the Stack Global Config Mode.
ARP Access-List Config Mode	Switch (Config-arp-access-list)#	Contains commands to add ARP ACL rules in an ARP Access List.

Table 6 explains how to enter or exit each mode.

Table 6. CLI Mode Access and Exit

Command Mode	Access Method	Exit or Access Previous Mode
User EXEC	This is the first level of access.	To exit, enter **`logout`**.
Privileged EXEC	From the User EXEC mode, enter **`enable`**.	To exit to the User EXEC mode, enter **`exit`** or press **`Ctrl-Z.`**
Global Config	From the Privileged EXEC mode, enter **`configure.`**	To exit to the Privileged EXEC mode, enter **`exit`**, or press **`Ctrl-Z`**.
VLAN Config	From the Privileged EXEC mode, enter **`vlan database.`**	To exit to the Privileged EXEC mode, enter **`exit`**, or press **`Ctrl-Z`**.
Interface Config	From the Global Config mode, enter **`interface`** *`<unit/slot/port>`* or **`interface loopback`** *`<id>`* or **`interface tunnel`** *`<id>`*	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Line Config	From the Global Config mode, enter **`lineconfig`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Policy-Map Config	From the Global Config mode, enter **`policy-map <name> in`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Policy-Class-Map Config	From the Policy Map mode enter **`class`**.	To exit to the Policy Map mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.

Table 6. CLI Mode Access and Exit (continued)

Command Mode	Access Method	Exit or Access Previous Mode
Class-Map Config	From the Global Config mode, enter **`class-map`**, and specify the optional keyword *`ipv4`* to specify the Layer 3 protocol for this class. See "class-map" on page 5-12 for more information.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Ipv6-Class-Map Config	From the Global Config mode, enter **`class-map`** and specify the optional keyword *`ipv6`* to specify the Layer 3 protocol for this class. See "class-map" on page 5-12 for more information.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Router OSPF Config	From the Global Config mode, enter **`router ospf`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Router OSPFv3 Config	From the Global Config mode, enter **`ipv6 router ospf`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Router RIP Config	From the Global Config mode, enter **`router rip`**.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Router BGP Config	From the Global Config mode, enter **`router bgp`** <*`asnumber`*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
MAC Access-list Config	From the Global Config mode, enter **`mac access-list extended`** <*`name`*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
TACACS Config	From the Global Config mode, enter **`tacacs-server host`** <*`ip-addr`*>, where <*`ip-addr`*> is the IP address of the TACACS server on your network.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
DHCP Pool Config	From the Global Config mode, enter **`ip dhcp pool`** <*`pool-name`*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.

Table 6. CLI Mode Access and Exit (continued)

Command Mode	Access Method	Exit or Access Previous Mode
DHCPv6 Pool Config	From the Global Config mode, enter **`ip dhcpv6 pool`** <*`pool-name`*>.	To exit to the Global Config mode, enter **`exit`**. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
Stack Global Config Mode	From the Global Config mode, enter the **`stack`** command.	To exit to the Global Config mode, enter the **`exit`** command. To return to the Privileged EXEC mode, enter **`Ctrl-Z`**.
ARP Access-List Config Mode	From the Global Config mode, enter the `arp access-list command`.	To exit to the Global Config mode, enter the `exit` command. To return to the Privileged EXEC mode, enter `Ctrl-Z`.

Command Completion and Abbreviation

Command completion finishes spelling the command when you type enough letters of a command to uniquely identify the command keyword. Once you have entered enough letters, press the SPACEBAR or TAB key to complete the word.

Command abbreviation allows you to execute a command when you have entered there are enough letters to uniquely identify the command. You must enter all of the required keywords and parameters before you enter the command.

CLI Error Messages

If you enter a command and the system is unable to execute it, an error message appears. Table 7 describes the most common CLI error messages.

Table 7. CLI Error Messages

Message Text	Description
% Invalid input detected at '^' marker.	Indicates that you entered an incorrect or unavailable command. The carat (^) shows where the invalid text is detected. This message also appears if any of the parameters or values are not recognized.

Table 7. CLI Error Messages

Message Text	Description
Command not found / Incomplete command. Use ? to list commands.	Indicates that you did not enter the required keywords or values.
Ambiguous command	Indicates that you did not enter enough letters to uniquely identify the command.

CLI Line-Editing Conventions

Table 8 describes the key combinations you can use to edit commands or increase the speed of command entry. You can access this list from the CLI by entering **`help`** from the User or Privileged EXEC modes.

Table 8. CLI Editing Conventions

Key Sequence	Description
DEL or Backspace	Delete previous character
Ctrl-A	Go to beginning of line
Ctrl-E	Go to end of line
Ctrl-F	Go forward one character
Ctrl-B	Go backward one character
Ctrl-D	Delete current character
Ctrl-U, X	Delete to beginning of line
Ctrl-K	Delete to end of line
Ctrl-W	Delete previous word
Ctrl-T	Transpose previous character
Ctrl-P	Go to previous line in history buffer
Ctrl-R	Rewrites or pastes the line
Ctrl-N	Go to next line in history buffer
Ctrl-Y	Prints last deleted character
Ctrl-Q	Enables serial flow
Ctrl-S	Disables serial flow
Ctrl-Z	Return to root command prompt
Tab, <SPACE>	Command-line completion

Table 8. CLI Editing Conventions (continued)

Key Sequence	Description
Exit	Go to next lower command prompt
?	List available commands, keywords, or parameters

Using CLI Help

Enter a question mark (?) at the command prompt to display the commands available in the current mode.

```
(switch) >?

enable                   Enter into user privilege mode.
help                     Display help for various special keys.
logout                   Exit this session. Any unsaved changes are lost.
ping                     Send ICMP echo packets to a specified IP address.
quit                     Exit this session. Any unsaved changes are lost.
show                     Display Switch Options and Settings.
telnet                   Telnet to a remote host.
```

Enter a question mark (?) after each word you enter to display available command keywords or parameters.

```
(switch) #network ?

javamode                 Enable/Disable.
mgmt_vlan                Configure the Management VLAN ID of the switch.
parms                    Configure Network Parameters of the router.
protocol                 Select DHCP, BootP, or None as the network config
                         protocol.
```

If the help output shows a parameter in angle brackets, you must replace the parameter with a value.

```
(switch) #network parms ?

<ipaddr>                 Enter the IP address.
```

If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                     Press Enter to execute the command
```

You can also enter a question mark (?) after typing one or more characters of a word to list the available command or parameters that begin with the letters, as shown in the following example:

```
(switch) #show m?

mac-addr-table           mac-address-table        monitor
```

Accessing the CLI

You can access the CLI by using a direct console connection or by using a telnet or SSH connection from a remote management host.

For the initial connection, you must use a direct connection to the console port. You cannot access the system remotely until the system has an IP address, subnet mask, and default gateway. You can set the network configuration information manually, or you can configure the system to accept these settings from a BOOTP or DHCP server on your network. For more information, see "Network Interface Commands" on page 7-4.

Chapter 2
Stacking Commands

The Stacking Commands chapter includes the following sections:

Note: The commands in this chapter are in two functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

The Primary Management Unit is the unit that controls the stack.

Dedicated Port Stacking

This section describes the commands you use to configure dedicated port stacking.

stack

This command sets the mode to Stack Global Config.

Format	`stack`
Mode	Global Config

member

This command configures a switch. The *`<unit>`* is the switch identifier of the switch to be added/removed from the stack. The *`<switchindex>`* is the index into the database of the supported switch types, indicating the type of the switch being preconfigured. The switch index is a 32-bit integer. This command is executed on the Primary Management Unit.

Format	**`member`** *`<unit> <switchindex>`*
Mode	Stack Global Config

Note: Switch index can be obtained by executing the show supported switchtype command in User EXEC mode.

no member

This command removes a switch from the stack. The *`<unit>`* is the switch identifier of the switch to be removed from the stack. This command is executed on the Primary Management Unit.

Format	**`no member`** *`<unit>`*
Mode	Stack Global Config

switch priority

This command configures the ability of a switch to become the Primary Management Unit. The *`<unit>`* is the switch identifier. The *`<value>`* is the preference parameter that allows the user to specify, priority of one backup switch over another. The range for priority is 1 to 15. The switch with the highest priority value will be chosen to become the Primary Management Unit if the active Primary Management Unit fails. The switch priority defaults to the hardware management preference value 1. Switches that do not have the hardware capability to become the Primary Management Unit are not eligible for management.

Default	enabled
Format	**switch** *<unit>* **priority** *<value>*
Mode	Global Config

switch renumber

This command changes the switch identifier for a switch in the stack. The `<oldunit>` is the current switch identifier on the switch whose identifier is to be changed. The `<newunit>` is the updated value of the switch identifier. Upon execution, the switch will be configured with the configuration information for the new switch, if any. The old switch configuration information will be retained, however the old switch will be operationally unplugged. This command is executed on the Primary Management Unit.

Note: If the management unit is renumbered, then the running configuration is no longer applied (i.e. the stack acts as if the configuration had been cleared)

Format	**`switch`** *`<oldunit>`* **`renumber`** *`<newunit>`*
Mode	Global Config

movemanagement

This command moves the Primary Management Unit functionality from one switch to another. The `<fromunit>` is the switch identifier on the current Primary Management Unit. The `<tounit>` is the switch identifier on the new Primary Management Unit. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new Primary Management Unit. After the reload is complete, all stack management capability must be performed on the new Primary Management Unit. To preserve the current configuration across a stack move, execute the `copy system:running-config` `nvram:startup-config` (in Privileged EXEC) command before performing the stack move. A stack move causes all routes and layer 2 addresses to be lost. This command is executed on the Primary Management Unit. The system prompts you to confirm the management move.

Format	**`movemanagement`** *`<fromunit> <tounit>`*
Mode	Stack Global Config

slot

This command configures a slot in the system. The *`<unit/slot>`* is the slot identifier of the slot. The *`<cardindex>`* is the index into the database of the supported card types, indicating the type of the card being preconfigured in the specified slot. The card index is a 32-bit integer. If a card is currently present in the slot that is unconfigured, the configured information will be deleted and the slot will be re-configured with default information for the card.

Format	**`slot`** *`<unit/slot> <cardindex>`*
Mode	Global Config

> **Note:** Card index can be obtained by executing show supported cardtype command in User EXEC mode.

no slot

This command removes configured information from an existing slot in the system.

Format	**`no slot`** *`<unit/slot> <cardindex>`*
Mode	Global Config

> **Note:** Card index can be obtained by executing show supported cardtype command in User EXEC mode.

set slot disable

This command configures the administrative mode of the slot(s). If you specify *`[all]`*, the command is applied to all slots, otherwise the command is applied to the slot identified by *`<unit/slot>`*.

If a card or other module is present in the slot, this administrative mode will effectively be applied to the contents of the slot. If the slot is empty, this administrative mode will be applied to any module that is inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as "unplugged" on management screens.

Format	**`set slot disable`** *`[<unit/slot>	all]`*
Mode	Global Config

no set slot disable

This command unconfigures the administrative mode of the slot(s). If you specify *`[all]`*, the command removes the configuration from all slots, otherwise the configuration is removed from the slot identified by *`<unit/slot>`*.

If a card or other module is present in the slot, this administrative mode removes the configuration from the contents of the slot. If the slot is empty, this administrative mode removes the configuration from any module inserted into the slot. If a card is disabled, all the ports on the device are operationally disabled and shown as "unplugged" on management screens.

Format	**`no set slot disable`** *`[<unit/slot>	all]`*
Mode	Global Config

set slot power

This command configures the power mode of the slot(s) and allows power to be supplied to a card located in the slot. If you specify *`[all]`*, the command is applied to all slots, otherwise the command is applied to the slot identified by *`<unit/slot>`*.

Use this command when installing or removing cards. If a card or other module is present in this slot, the power mode is applied to the contents of the slot. If the slot is empty, the power mode is applied to any card inserted into the slot.

Format	**`set slot power`** *`[<unit/slot>	all]`*
Mode	Global Config

no set slot power

This command unconfigures the power mode of the slot(s) and prohibits power from being supplied to a card located in the slot. If you specify *`[all]`*, the command prohibits power to all slots, otherwise the command prohibits power to the slot identified by *`<unit/slot>`*.

Use this command when installing or removing cards. If a card or other module is present in this slot, power is prohibited to the contents of the slot. If the slot is empty, power is prohibited to any card inserted into the slot.

Format	**`no set slot power`** *`[<unit/slot>	all]`*
Mode	Global Config

reload (Stack)

This command resets the entire stack or the identified *`<unit>`*`.` The *`<unit>`* is the switch identifier. The system prompts you to confirm that you want to reset the switch.

Format	**`reload`** *`[<unit>]`*
Mode	User EXEC

show slot

This command displays information about all the slots in the system or for a specific slot.

Format	**`show slot`** *`[<unit/slot>]`*
Mode	User EXEC

Term	Definition
Slot	The slot identifier in a <*unit/slot*> format.
Slot Status	The slot is empty, full, or has encountered an error
Admin State	The slot administrative mode is enabled or disabled.
Power State	The slot power mode is enabled or disabled.
Configured Card Model Identifier	The model identifier of the card preconfigured in the slot. Model Identifier is a 32-character field used to identify a card.
Pluggable	Cards are pluggable or non-pluggable in the slot.
Power Down	Indicates whether the slot can be powered down.

If you supply a value for *`<unit/slot>`*, the following additional information appears:

Term	Definition
Inserted Card Model Identifier	The model identifier of the card inserted in the slot. Model Identifier is a 32-character field used to identify a card. This field is displayed only if the slot is full.
Inserted Card Description	The card description. This field is displayed only if the slot is full.
Configured Card Description	The card description of the card preconfigured in the slot.

show supported cardtype

This commands displays information about all card types or specific card types supported in the system.

Format	**`show supported cardtype`** *`[<cardindex>]`*
Mode	User EXEC

If you do not supply a value for *`<cardindex>`*, the following output appears:

Term	Definition
Card Index (CID)	The index into the database of the supported card types. This index is used when preconfiguring a slot.
Card Model Identifier	The model identifier for the supported card type.

If you supply a value for `<cardindex>`, the following output appears:

Term	Definition
Card Type	The 32-bit numeric card type for the supported card.
Model Identifier	The model identifier for the supported card type.
Card Description	The description for the supported card type.

show switch

This command displays information about all units in the stack or a single unit when you specify the unit value.

Format	`show switch [<unit>]`
Mode	Privileged EXEC

Term	Definition
Switch	The unit identifier assigned to the switch.

When you do not specify a value for `<unit>`, the following information appears:

Term	Definition
Management Status	Indicates whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.
Preconfigured Model Identifier	The model identifier of a preconfigured switch ready to join the stack. The Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Plugged-In Model Identifier	The model identifier of the switch in the stack. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values for this state are: OK, Unsup ported, Code Mismatch, Config Mismatch, or Not Present.
Code Version	The detected version of code on this switch.

When you specify a value for `<unit>`, the following information appears:

Term	Definition
Management Status	Indicates whether the switch is the Primary Management Unit, a stack member, or the status is unassigned.
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.
Admin Management Preference	The administrative management preference value assigned to the switch. This preference value indicates how likely the switch is to be chosen as the Primary Management Unit.
Switch Type	The 32-bit numeric switch type.
Model Identifier	The model identifier for this switch. Model Identifier is a 32-character field assigned by the device manufacturer to identify the device.
Switch Status	The switch status. Possible values are OK, Unsupported, Code Mismatch, Config Mismatch, or Not Present.
Switch Description	The switch description.
Expected Code Version	The expected code version.
Detected Code Version	The version of code running on this switch. If the switch is not present and the data is from pre-configuration, then the code version is “None”.
Detected Code in Flash	The version of code that is currently stored in FLASH memory on the switch. This code executes after the switch is reset. If the switch is not present and the data is from pre-configuration, then the code version is “None”.
Up Time	The system up time.

show supported switchtype

This commands displays information about all supported switch types or a specific switch type.

Format	**`show supported switchtype`** *`[<switchindex>]`*
Mode	User EXEC Privileged EXEC

If you do not supply a value for *`<switchindex>`*, the following output appears:

Term	Definition
Switch Index (SID)	The index into the database of supported switch types. This index is used when preconfiguring a member to be added to the stack.
Model Identifier	The model identifier for the supported switch type.
Management Preference	The management preference value of the switch type.
Code Version	The code load target identifier of the switch type.

If you supply a value for *`<switchindex>`*, the following output appears:

Term	Definition
Switch Type	The 32-bit numeric switch type for the supported switch.
Model Identifier	The model identifier for the supported switch type.
Switch Description	The description for the supported switch type.

Front Panel Stacking Commands

This section describes the commands you use to view and configure front panel stacking information.

stack-port

This command sets front panel stacking per port to either *`stack`* or *`ethernet`* mode.

Default	stack
Format	**`stack-port`** *`<unit/slot/port> [{ethernet	stack}]`*
Mode	Stack Global Config

show stack-port

This command displays summary stack-port information for all interfaces.

Format	`show stack-port`
Mode	Privileged EXEC

Term	Definition
QOS Mode	Front Panel Stacking QOS Mode for all Interfaces.

For Each Interface:

Term	Definition
Unit	The unit number.
Interface	The slot and port numbers.
Configured Stack Mode	Stack or Ethernet.
Running Stack Mode	Stack or Ethernet.
Link Status	Status of the link.
Link Speed	Speed (Gbps) of the stack port link.

show stack-port counters

This command displays summary data counter information for all interfaces.

Format	`show stack-port counters`
Mode	Privileged EXEC

Term	Definition
Unit	The unit number.
Interface	The slot and port numbers.
Tx Data Rate	Trashing data rate in megabits per second on the stacking port.
Tx Error Rate	Platform-specific number of transmit errors per second.

Term	Definition
Tx Total Error	Platform-specific number of total transmit errors since power-up.
Rx Data Rate	Receive data rate in megabits per second on the stacking port.
Rx Error Rate	Platform-specific number of receive errors per second.
Rx Total Errors	Platform-specific number of total receive errors since power-up.

show stack-port diag

This command shows front panel stacking diagnostics for each port and is only intended for Field Application Engineers (FAEs) and developers. An FAE will advise on the necessity to run this command and capture this information.

Format	`show stack-port diag`
Mode	Privileged EXEC

Term	Definition
Unit	The unit number.
Interface	The slot and port numbers.
Diagnostic Entry1	80 character string used for diagnostics.
Diagnostic Entry2	80 character string used for diagnostics.
Diagnostic Entry3	80 character string used for diagnostics.

Non-Stop Forwarding Commands

Non-stop forwarding allows the stack units to continue to forward packets if the stack management unit restarts because of a power failure, hardware failure, or software fault.

nsf

This command enables non-stop forwarding.

Default	Enabled
Format	`nsf`
Mode	Stack Global Config

no nsf

This command disables non-stop forwarding.

Format	`no nsf`
Mode	Stack Global Config

show nsf

This command shows the status of non-stop forwarding.

Format	`show nsf`
Mode	Privileged EXEC

Example:

```
(Switch)#show nsf
Administrative Status.......................... Enable
Operational Status............................. Enable
Last Startup Reason............................ Warm Auto-Restart
Time Since Last Restart........................ 0 days 16 hrs 52 mins 55 secs
Restart In Progress............................ No
Warm Restart Ready............................. Yes
Copy of Running Configuration to Backup Unit:
Status...................................... Stale
Time Since Last Copy........................ 0 days 4 hrs 53 mins 22 secs
Time Until Next Copy........................ 28 seconds
Unit NSF Support
---- -----------
1 Yes
2 Yes
3 Yes
```

show checkpoint statistics

This command displays the statistics for the checkpointing process.

Format	`show checkpoint statistics`
Mode	Privileged EXEC

Example:

```
(Switch)#show checkpoint statistics
Messages Checkpointed.....................6708
Bytes Checkpointed........................894305
Time Since Counters Cleared...............3d 01:05:09
Checkpoint Message Rate...................0.025 msg/sec
Last 10-second Message Rate...............0 msg/sec
Highest 10-second Message Rate............8 msg/sec
```

clear checkpoint statistics

This command clears the statistics for the checkpointing process.

Format	`clear checkpoint statistics`
Mode	Privileged EXEC

Stack Firmware Synchronization Commands

Stack firmware synchronization provides an automatic mechanism to synchronize the firmware on stack members whose firmware version differs from the version running on the stack manager. This operation can result in either an upgrade or downgrade of firmware on the mismatched stack member. However, this operation does not attempt to synchronize the stack to the latest firmware in the stack.

During firmware transfer and upgrade, operations such as code download and move management can result in undesirable behavior, such as firmware corruption on a code mismatched stack member. As a result, you receive an error if you try to access the following operations from the user interface during stack firmware synchronization:

- Move management
- Unit renumbering
- Code download

- Delete image
- Update bootcode
- Clear config

A reboot operation is allowed during stack firmware synchronization.

If the firmware is corrupted during stack firmware synchronization, manual intervention by the administrator is required to restore the switch to working condition.

During stack firmware synchronization, traps are generated on start, completion, or failure.

Note:

- Non-deterministic upgrade behavior

  On bootup, the image that gets synchronized depends on the one that becomes the manager. Which code version the new stack synchronizes to is fully deterministic, but might not be obvious to the user as it depends entirely on which unit becomes the manager. This might be decided by a MAC address comparison. If the administrator wants a particular version to be used by the stack, he should first ensure that this particular unit becomes stack manager.

- Bootcode Upgrades

  Bootcode upgrades are not initiated by the stack firmware synchronization.

boot auto-copy-sw

This command enables or disables stack firmware synchronization.

Default	Disabled
Format	`boot auto-copy-sw`
Mode	Privileged EXEC

no boot auto-copy-sw

This command disables stack firmware synchronization.

Format	`no boot auto-copy-sw`
Mode	Privileged EXEC

boot auto-copy-sw trap

This command sends SNMP traps related to stack firmware synchronization.

Default	Enabled
Format	`boot auto-copy-sw trap`
Mode	Privileged EXEC

no boot auto-copy-sw trap

This command disables sending SNMP traps related to stack firmware synchronization.

Format	`no boot auto-copy-sw trap`
Mode	Privileged EXEC

boot auto-copy-sw allow-downgrade

This command enables downgrading the firmware version on the stack member if the firmware version on the manager is older than the firmware version on the member.

Default	Enabled
Format	`boot auto-copy-sw allow-downgrade`
Mode	Privileged EXEC

no boot auto-copy-sw allow-downgrade

This command disables downgrading the image.

Format	`no boot auto-copy-sw allow-downgrade`
Mode	Privileged EXEC

show auto-copy-sw

This command displays the stack firmware synchronization configuration status.

Format	`show auto-copy-sw`
Mode	Privileged EXEC

Example:

```
(Switch)#show auto-copy-sw
Stack Firmware Synchronization
Synchronization: Enabled
SNMP Trap status: Enabled
Allow Downgrade: Enabled
```

Chapter 3
Switching Commands

This chapter describes the switching commands available in the managed switch CLI.

The Switching Commands chapter includes the following sections:

⚠ **Warning:** The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Port Configuration Commands

This section describes the commands you use to view and configure port settings.

interface

This command gives you access to the Interface Config mode, which allows you to enable or modify the operation of an interface (port).

Format	`interface <unit/slot/port>`
Mode	Global Config

interface range

This command gives you access to a range of port interfaces, allowing the same port configuration to be applied to a set of ports.

Format	**interface range** *<unit/slot/port>-<unit/slot/port>*
Mode	Global Config

interface vlan

This command gives you access to the vlan virtual interface mode, which allows certain port configurations (for example, the IP address) to be applied to the VLAN interface. Type a question mark (?) after entering the interface configuration mode to see the available options.

Format	interface vlan <*vlan id*>
Mode	Global Config

interface lag

This command gives you access to the LAG (link aggregation, or port channel) virtual interface, which allows certain port configurations to be applied to the LAG interface. Type a question mark (?) after entering the interface configuration mode to see the available options.

Note: The IP address cannot be assigned to a LAG virtual interface. The interface must be put under a VLAN group and an IP address assigned to the VLAN group.

Format	interface lag <*lag id*>
Mode	Global Config

auto-negotiate

This command enables automatic negotiation on a port.

Default	enabled

Format	`auto-negotiate`
Mode	Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

> **Note:** Automatic sensing is disabled when automatic negotiation is disabled.

auto-negotiate all

Format	`no auto-negotiate`
Mode	Interface Config

This command enables automatic negotiation on all ports.

Default	enabled
Format	`auto-negotiate all`
Mode	Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format	`no auto-negotiate all`
Mode	Global Config

description

Use this command to create an alpha-numeric description of the port.

Format	`description <`*`description`*`>`
Mode	Interface Config

mtu

Use the **`mtu`** command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the **`mtu`** command to configure jumbo frame support for physical and port-channel (LAG) interfaces. For the standard 7000 series implementation, the MTU size is a valid integer between 1522 - 9216 for tagged packets and a valid integer between 1518 - 9216 for untagged packets.

> **Note:** To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet (IP Header + IP payload), see "ip mtu" on page 4-12.

Default	1518 (untagged)
Format	`mtu <`*`1518-9216`*`>`
Mode	Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format	`no mtu`
Mode	Interface Config

shutdown

This command disables a port.

> **Note:** You can use the `shutdown` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown`
Mode	Interface Config

no shutdown

This command enables a port.

Format	`no shutdown`
Mode	Interface Config

shutdown all

This command disables all ports.

> **Note:** You can use the `shutdown all` command on physical and port-channel (LAG) interfaces, but not on VLAN routing interfaces.

Default	enabled
Format	`shutdown all`
Mode	Global Config

no shutdown all

This command enables all ports.

Format	`no shutdown all`
Mode	Global Config

speed

This command sets the speed and duplex setting for the interface.

Format	`speed {<100 | 10> <half-duplex | full-duplex>}`
Mode	Interface Config

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

speed all

This command sets the speed and duplex setting for all interfaces.

Format	`speed all {<100 | 10> <half-duplex | full-duplex>}`
Mode	Global Config

Acceptable Values	Definition
100h	100BASE-T half duplex
100f	100BASE-T full duplex
10h	10BASE-T half duplex
10f	10BASE-T full duplex

show port

This command displays port information.

Format	`show port {<unit/slot/port> | all}`
Mode	Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • **Mirror** - this port is a monitoring port. For more information, see "Port Mirroring" on page 3-115. • **PC Mbr**- this port is a member of a port-channel (LAG). • **Probe** - this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed is set from the auto-negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format	`show port protocol {<groupid> | all}`
Mode	Privileged EXEC

Term	Definition
Group Name	The group name of an entry in the Protocol-based VLAN table.
Group ID	The group identifier of the protocol group.
Protocol(s)	The type of protocol(s) for this group.
VLAN	The VLAN associated with this Protocol Group.
Interface(s)	Lists the unit/slot/port interface(s) that are associated with this Protocol Group.

show port description

This command displays the port description for every port.

Format	`show port description <`*`unit/slot/port`*`>`
Mode	Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes
Description	Shows the port description configured via the “description” command

show port status

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated group.

Format	`show port status {<`*`unit/slot/port`*`> | `*`all`*`}`
Mode	Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Media Type	“Copper” or “Fiber” for combo port.
STP Mode	Indicate the spanning tree mode of the port.

Term	Definition
Physical Mode	Either “Auto” or fixed speed and duplex mode.
Physical Status	The actual speed and duplex mode.
Link Status	Whether the link is Up or Down.
Loop Status	Whether the port is in loop state or not.
Partner Flow Control	Whether the remote side is using flow control or not.

Spanning Tree Protocol (STP) Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default	enabled
Format	`spanning-tree`
Mode	Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format	`no spanning-tree`
Mode	Global Config

spanning-tree bpdufilter default

Use this command to enable BPDU Filter on all the edge port interfaces.

Default	disabled
Format	`spanning-tree bpdufilter`
Mode	Global Config

no spanning-tree bpdufilter default

Use this command to disable BPDU Filter on all the edge port interfaces.

Default	enabled
Format	`no spanning-tree bpdufilter default`
Mode	Global Config

spanning-tree bpduflood

Use this command to enable BPDU Flood on the interface.

Default	disabled
Format	`spanning-tree bpduflood`
Mode	Interface Config

no spanning-tree bpduflood

Use this command to disable BPDU Flood on the interface.

Format	`no spanning-tree bpduflood`
Mode	Interface Config

spanning-tree bpduguard

Use this command to enable BPDU Guard on the switch.

Default	disabled
Format	`spanning-tree bpduguard`
Mode	Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the switch.

Format	`no spanning-tree bpduguard`
Mode	Global Config

spanning-tree bpdumigrationcheck

Use this command to force a transmission of rapid spanning tree (RSTP) and multiple spanning tree (MSTP) BPDUs. Use the *`<unit/slot/port>`* parameter to transmit a BPDU from a specified interface, or use the *`all`* keyword to transmit BPDUs from all interfaces. This command forces the BPDU transmission when you execute it, so the command does not change the system configuration or have a “no” version.

Format	`spanning-tree bpdumigrationcheck {<unit/slot/port> | all}`
Mode	Global Config

spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The *`<name>`* is a string of up to 32 characters.

Default	base MAC address in hexadecimal notation
Format	`spanning-tree configuration name <name>`
Mode	Global Config

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format	`no spanning-tree configuration name`
Mode	Global Config

spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default	0
Format	`spanning-tree configuration revision` *<0-65535>*
Mode	Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format	`no spanning-tree configuration revision`
Mode	Global Config

spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Default	`enabled`
Format	`spanning-tree edgeport`
Mode	Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format	`no spanning-tree edgeport`
Mode	Interface Config

spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value.

Default	802.1s
Format	`spanning-tree forceversion` *<802.1d | 802.1s | 802.1w>*
Mode	Global Config

- Use 802.1d to specify that the switch transmits ST BPDUs rather than MST BPDUs (IEEE 802.1d functionality supported).
- Use 802.1s to specify that the switch transmits MST BPDUs (IEEE 802.1s functionality supported).
- Use 802.1w to specify that the switch transmits RST BPDUs rather than MST BPDUs (IEEE 802.1w functionality supported).

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value.

Format	`no spanning-tree forceversion`
Mode	Global Config

spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to “(Bridge Max Age / 2) + 1”.

Default	15
Format	`spanning-tree forward-time` *<4-30>*
Mode	Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree forward-time`
Mode	Global Config

spanning-tree guard

This command selects whether loop guard or root guard is enabled on an interface. If neither is enabled, then the port operates in accordance with the multiple spanning tree protocol.

Default	none
Format	`spanning-tree guard` *`{ none	root	loop }`*
Mode	Interface Config

no spanning-tree guard

This command disables loop guard or root guard on the interface.

Format	`no spanning-tree guard`
Mode	Interface Config

spanning-tree tcnguard

This command enables the propagation of received topology change notifications and topology changes to other ports..

Default	disable
Format	`spanning-tree tcnguard`
Mode	Global Config

no spanning-tree tcnguard

This command disables the propagation of received topology change notifications and topology changes to other ports.

Format	`no spanning-tree tcnguard`
Mode	Global Config

spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to *2 x (Bridge Forward Delay - 1)*.

Default	20
Format	`spanning-tree max-age` *`<6-40>`*
Mode	Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-age`
Mode	Global Config

spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Default	20
Format	`spanning-tree max-hops` *`<1-127>`*
Mode	Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree max-hops`
Mode	Global Config

spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an *`<mstid>`* parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the *`<mstid>`*, the configurations are done for the common and internal spanning tree instance.

If you specify the **cost** option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the *`<mstid>`* parameter. You can set the path cost as a number in the range of 1 to 200000000 or **auto**. If you select **auto** the path cost value is set based on Link Speed.

If you specify the **external-cost** option, this command sets the external-path cost for MST instance ‘0’ i.e. CIST instance. You can set the external cost as a number in the range of 1 to 200000000 or **auto**. If you specify auto, the external path cost value is set based on Link Speed.

If you specify the **port-priority** option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the *`<mstid>`* parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default	• cost—auto • external-cost—auto • port-priority—128
Format	`spanning-tree mst` *`<mstid> {{cost <1-200000000> | auto} | {external-cost <1-200000000> | auto} | port-priority <0-240>}`*
Mode	Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an `<mstid>` parameter that corresponds to an existing multiple spanning tree instance, you are configuring that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the `<mstid>`, you are configuring the common and internal spanning tree instance.

If the you specify **cost**, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the `<mstid>` parameter, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **external-cost**, this command sets the external path cost for this port for mst ‘0’ instance, to the default value, i.e. a path cost value based on the Link Speed.

If you specify **port-priority**, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the `<mstid>` parameter, to the default value.

Format	`no spanning-tree mst <mstid> <cost	external-cost	port-priority>`
Mode	Interface Config

spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter `<mstid>` is a number within a range of 1 to 4094, that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Default	none
Format	`spanning-tree mst instance <mstid>`
Mode	Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format	`no spanning-tree mst instance <mstid>`
Mode	Global Config

spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the `<mstid>`, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Default	32768
Format	`spanning-tree mst priority <mstid> <0-61440>`
Mode	Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the `<mstid>`, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format	`no spanning-tree mst priority <mstid>`
Mode	Global Config

spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance. The vlan range can be specified as a list or as a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash ("-").

Format	`spanning-tree mst vlan <mstid> <vlanid>`
Mode	Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format	`no spanning-tree mst vlan <mstid> <vlanid>`
Mode	Global Config

spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default	disabled
Format	`spanning-tree port mode`
Mode	Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format	`no spanning-tree port mode`
Mode	Interface Config

spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default	disabled
Format	`spanning-tree port mode all`
Mode	Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format	`no spanning-tree port mode all`
Mode	Global Config

spanning-tree edgeport all

This command specifies that every port is an Edge Port within the common and internal spanning tree. This allows all ports to transition to Forwarding State without delay.

Format	`spanning-tree edgeport all`
Mode	Global Config

no spanning-tree edgeport all

This command disables Edge Port mode for all ports within the common and internal spanning tree.

Format	`no spanning-tree edgeport all`
Mode	Global Config

spanning-tree bpduforwarding

Normally a switch will not forward Spanning Tree Protocol (STP) BPDU packets if STP is disabled. However, if in some network setup, the user wishes to forward BDPU packets received from other network devices, this command can be used to enable the forwarding.

Default	2
Format	`spanning-tree bpduforwarding`
Mode	Global Config

no spanning-tree bpduforwarding

This command will cause the STP BPDU packets received from the network to be dropped if STP is disabled.

Format	`no spanning-tree bpduforwarding`
Mode	Global Config

show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format	`show spanning-tree`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.

Term	Definition
Topology Change Count	Number of times changed.
Topology Change	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Root Port Max Age	Derived value.
Root Port Bridge Forward Delay	Derived value.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
Bridge Max Hops	Bridge max-hops count for the device.
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.
Associated FIDs	List of forwarding database identifiers currently associated with this instance.
Associated VLANs	List of VLAN IDs currently associated with this instance.

show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format	`show spanning-tree brief`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.
Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *<unit/slot/port>* is the desired switch port. The following details are displayed on execution of the command.

Format	`show spanning-tree interface` *<unit/slot/port>*
Mode	• Privileged EXEC • User EXEC

Term	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
BPDU Guard Effect	Enabled or disabled.
Root Guard	Enabled or disabled.
Loop Guard	Enabled or disabled.
TCN Guard	Enable or disable the propagation of received topology change notifications and topology changes to other ports.
BPDU Filter Mode	Enabled or disabled.
BPDU Flood Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for ‘edge delay’ time, to become an edge port and transition to forwarding faster.
Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.

Term	Definition
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter `<mstid>` is a number that corresponds to the desired existing multiple spanning tree instance. The `<unit/slot/port>` is the desired switch port.

Format `show spanning-tree mst port detailed <mstid> <unit/slot/port>`

Mode

- Privileged EXEC
- User EXEC

Term	Definition
MST Instance ID	The ID of the existing MST instance.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
PortForwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.

Term	Definition
Designated Root	The Identifier of the designated root for this port.
Root Path Cost	The path cost to get to the root bridge for this instance. The root path cost is zero if the bridge is the root bridge for that instance.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a "blocking" state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

If you specify 0 (defined as the default CIST ID) as the `<mstid>`, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The *`<unit/slot/port>`* is the desired switch port. In this case, the following are displayed.

Term	Definition
Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.

Term	Definition
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Root Path Cost	The root path cost to the LAN by the port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.
Loop Inconsistent State	The current loop inconsistent state of this port in this MST instance. When in loop inconsistent state, the port has failed to receive BPDUs while configured with loop guard enabled. Loop inconsistent state maintains the port in a "blocking" state until a subsequent BPDU is received.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter *<mstid>* indicates a particular MST instance. The parameter {*<unit/slot/port>* | *all*} indicates the desired switch port or all ports.

If you specify 0 (defined as the default CIST ID) as the *<mstid>*, the status summary displays for one or all ports within the common and internal spanning tree.

Format	`show spanning-tree mst port summary` *<mstid> {<unit/slot/port> | all}*
Mode	• Privileged EXEC • User EXEC

Term	Definition
MST Instance ID	The MST instance associated with this port.
Interface	Valid slot and port number separated by forward slashes.
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst port summary active

This command displays settings for the ports within the specified multiple spanning tree instance that are active links.

Format	`show spanning-tree mst port summary` <mstid> active
Mode	• Privileged EXEC • User EXEC

Term	Definition
mstid	The ID of the existing MST instance.
Interface	`unit/slot/port`

Term	Definition
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.
Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not. This field is blank if the loop guard feature is not available.

show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format	`show spanning-tree mst summary`
Mode	• Privileged EXEC • User EXEC

Term	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • Associated FIDs • Associated VLANs	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format	`show spanning-tree summary`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Spanning Tree Adminmode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
BPDU Guard Mode	Enabled or disabled.
BPDU Filter Mode	Enabled or disabled.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <*vlanid*> corresponds to an existing VLAN ID.

Format	`show spanning-tree vlan <vlanid>`
Mode	• Privileged EXEC • User EXEC

Term	Definition
VLAN Identifier	The VLANs associated with the selected MST instance.
Associated Instance	Identifier for the associated multiple spanning tree instance or “CST” if associated with the common and internal spanning tree.

VLAN Commands

This section describes the commands you use to configure VLAN settings.

vlan database

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format	`vlan database`
Mode	Privileged EXEC

network mgmt_vlan

This command configures the Management VLAN ID.

Default	1
Format	`network mgmt_vlan` *<1-4093>*
Mode	Privileged EXEC

no network mgmt_vlan

This command sets the Management VLAN ID to the default.

Format	`no network mgmt_vlan`
Mode	Privileged EXEC

vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Format	`vlan <vlan-list>`
Mode	VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Format	`no vlan <vlan-list>`
Mode	VLAN Config

vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default	all
Format	`vlan acceptframe {vlanonly	all}`
Mode	Interface Config

no vlan acceptframe

This command resets the frame acceptance mode for the interface to the default value.

Format	`no vlan acceptframe`
Mode	Interface Config

vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	`vlan ingressfilter`
Mode	Interface Config

no vlan ingressfilter

This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	`no vlan ingressfilter`
Mode	Interface Config

vlan makestatic

This command changes a dynamically created VLAN (one that is created by GVRP registration) to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format	`vlan makestatic <2-4093>`
Mode	VLAN Config

vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Default	• VLAN ID 1 - default • other VLANS - blank string
Format	`vlan name <1-4093> <name>`
Mode	VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format	`no vlan name <1-4093>`
Mode	VLAN Config

vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format	`vlan participation {exclude	include	auto} <1-4093>`
Mode	Interface Config

Participation options are:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format	`vlan participation all` *`{exclude	include	auto} <1-4093>`*
Mode	Global Config

You can use the following participation options:

Participation Options	Definition
include	The interface is always a member of this VLAN. This is equivalent to registration fixed.
exclude	The interface is never a member of this VLAN. This is equivalent to registration forbidden.
auto	The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces.

Default	all
Format	`vlan port acceptframe all` *`{vlanonly	all}`*
Mode	Global Config

The modes defined as follows:

Mode	Definition
VLAN Only mode	Untagged frames or priority frames received on this interface are discarded.
Admit All mode	Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to Admit All. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format	`no vlan port acceptframe all`
Mode	Global Config

vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default	disabled
Format	`vlan port ingressfilter all`
Mode	Global Config

no vlan port ingressfilter all

This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format	`no vlan port ingressfilter all`
Mode	Global Config

vlan port pvid all

This command changes the VLAN ID for all interface.

Default	1
Format	`vlan port pvid all <1-4093>`
Mode	Global Config

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format	`no vlan port pvid` *`all`*
Mode	Global Config

vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`vlan port tagging all <`*`1-4093`*`>`
Mode	Global Config

no vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format	`no vlan port tagging all`
Mode	Global Config

vlan protocol group

This command adds protocol-based VLAN groups to the system. When it is created, the protocol group will be assigned a unique number (1-128) that will be used to identify the group in subsequent commands.

Format	`vlan protocol group <`*`1-128`*`>`
Mode	Global Config

no vlan protocol group

This command removes a protocol group.

Format	`no vlan protocol group <1-128>`
Mode	Global Config

vlan protocol group name

This command assigns a name to a protocol-based VLAN groups. The *groupname* variable can be a character string of 0 to 16 characters.

Format	`vlan protocol group name <1-128> <groupname>`
Mode	Global Config

no vlan protocol group name

This command removes the name from a protocol-based VLAN groups.

Format	`no vlan protocol group name <1-128>`
Mode	Global Config

vlan protocol group add protocol

This command adds the protocol to the protocol-based VLAN identified by groupid. Agroup may have more than one protocol associated with it. Each interface and protocolcombination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command fails and the protocol is not added to the group. The possible values for protocol-list includes the keywords ip, arp, and ipx and hexadecimal or decimal values ranging from 0x0600 (1536) to 0xFFFF (65535). The protocol list can accept up to 16 protocols separated by a comma.

Default	none
Format	`vlan protocol group add protocol <groupid> ethertype {<protocol-list>|arp|ip|ipx}`
Mode	Global Config

no vlan protocol group add protocol

This command removes the `<protocol>` from this protocol-based VLAN group that is identified by this `<groupid>`. The possible values for protocol are `ip, arp,` and `ipx`.

Format	`no vlan protocol group add protocol <groupid> ethertype {<protocol-list>|arp|ip|ipx}`
Mode	Global Config

protocol group

This command attaches a `<vlanid>` to the protocol-based VLAN identified by `<groupid>`. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

Default	none
Format	`protocol group <groupid> <vlanid>`
Mode	VLAN Config

no protocol group

This command removes the `<vlanid>` from this protocol-based VLAN group that is identified by this `<groupid>`.

Format	`no protocol group <groupid> <vlanid>`
Mode	VLAN Config

protocol vlan group

This command adds the physical interface to the protocol-based VLAN identified by `<groupid>`. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command fails and the interface(s) are not added to the group.

Default	none
Format	`protocol vlan group <groupid>`
Mode	Interface Config

no protocol vlan group

This command removes the interface from this protocol-based VLAN group that is identified by this `<groupid>`.

Format	`no protocol vlan group <groupid>`
Mode	Interface Config

protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by `<groupid>`. You can associate multiple interfaces with a group, but you can only associate each interface and protocol combination with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

Default	none
Format	`protocol vlan group all <groupid>`
Mode	Global Config

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this `<groupid>`.

Format	`no protocol vlan group all <groupid>`
Mode	Global Config

vlan pvid

This command changes the VLAN ID per interface.

Default	1
Format	`vlan pvid <1-4093>`
Mode	Interface Config

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format	`no vlan pvid`
Mode	Interface Config

vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Format	`vlan tagging <vlan-list>`
Mode	Interface Config

no vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The vlan-list contains VlanId's in range <1-4093>. Separate non-consecutive IDs with ',' and no spaces and no zeros in between the range; Use '-' for range.

Format	`no vlan tagging <vlan-list>`
Mode	Interface Config

vlan association subnet

This command associates a VLAN to a specific IP-subnet.

Format	`vlan association subnet <ipaddr> <netmask> <1-4093>`
Mode	VLAN Config

no vlan association subnet

This command removes association of a specific IP-subnet to a VLAN.

Format	`no vlan association subnet <ipaddr> <netmask>`
Mode	VLAN Config

vlan association mac

This command associates a MAC address to a VLAN.

Format	`vlan association mac <macaddr> <1-4093>`
Mode	VLAN database

no vlan association mac

This command removes the association of a MAC address to a VLAN.

Format	`no vlan association mac <macaddr>`
Mode	VLAN database

show vlan

This command displays a list of all configured VLAN.

Format	`show vlan`
Mode	• Privileged EXEC • User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).

show vlan <vlanid>

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number.

Format	`show vlan <vlanid>`
Mode	• Privileged EXEC • User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface	Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Term	Definition
Current	The degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured	The configured degree of participation of this port in this VLAN. The permissible values are: • **Include** - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude** - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect** - To allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging	The tagging behavior for this port in this VLAN. • **Tagged** - Transmit traffic for this VLAN as tagged frames. • **Untagged** - Transmit traffic for this VLAN as untagged frames.

show vlan brief

This command displays a list of all configured VLANs.

Format	`show vlan brief`
Mode	• Privileged EXEC • User EXEC

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of “Default.” This field is optional.
VLAN Type	Type of VLAN, which can be Default (VLAN ID = 1) or static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

show vlan port

This command displays VLAN port information.

Format	`show vlan port {<unit/slot/port>	all}`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.
Port VLAN ID	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Acceptable Frame Types	The types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.
GVRP	May be enabled or disabled.
Default Priority	The 802.1p priority assigned to tagged packets arriving on the port.

show vlan association subnet

This command displays the VLAN associated with a specific configured IP-Address and net mask. If no IP address and net mask are specified, the VLAN associations of all the configured IP-subnets are displayed.

Format	`show vlan association subnet [<ipaddr> <netmask>]`
Mode	Privileged EXEC

Term	Definition
IP Subnet	The IP address assigned to each interface.
IP Mask	The subnet mask.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

show vlan association mac

This command displays the VLAN associated with a specific configured MAC address. If no MAC address is specified, the VLAN associations of all the configured MAC addresses are displayed.

Format	`show vlan association mac` *[<macaddr>]*
Mode	Privileged EXEC

Term	Definition
MAC Address	A MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN.

Double VLAN Commands

This section describes the commands you use to configure double VLAN (DVLAN). Double VLAN tagging is a way to pass VLAN traffic from one customer domain to another through a Metro Core in a simple and cost effective manner. The additional tag on the traffic helps differentiate between customers in the MAN while preserving the VLAN identification of the individual customers when they enter their own 802.1Q domain.

dvlan-tunnel ethertype

This command configures the ether-type for all interfaces. The ether-type may have the values of *802.1Q*, *vMAN*, or *custom*. If the ether-type has a value of *custom*, the optional value of the custom ether type must be set to a value from 0 to 65535.

Default	vman
Format	`dvlan-tunnel ethertype` *`{802.1Q	vman	custom} [0-65535]`*
Mode	Global Config

mode dot1q-tunnel

This command is used to enable Double VLAN Tunneling on the specified interface.

Default	disabled
Format	`mode dot1q-tunnel`
Mode	Interface Config

no mode dot1q-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	`no mode dot1q-tunnel`
Mode	Interface Config

mode dvlan-tunnel

Use this command to enable Double VLAN Tunneling on the specified interface.

Note: When you use the `mode dvlan-tunnel` command on an interface, it becomes a service provider port. Ports that do not have double VLAN tunneling enabled are customer ports.

Default	disabled
Format	`mode dvlan-tunnel`
Mode	Interface Config

no mode dvlan-tunnel

This command is used to disable Double VLAN Tunneling on the specified interface. By default, Double VLAN Tunneling is disabled.

Format	`no mode dvlan-tunnel`
Mode	Interface Config

show dot1q-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format	`show dot1q-tunnel` *`[interface {<unit/slot/port>`* `|` *`all}]`*
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

show dvlan-tunnel

Use this command without the optional parameters to display all interfaces enabled for Double VLAN Tunneling. Use the optional parameters to display detailed information about Double VLAN Tunneling for the specified interface or all interfaces.

Format `show dvlan-tunnel [interface {<unit/slot/port> | all}]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Mode	The administrative mode through which Double VLAN Tunneling can be enabled or disabled. The default value for this field is disabled.
EtherType	A 2-byte hex EtherType to be used as the first 16 bits of the DVLAN tunnel. There are three different EtherType tags. The first is 802.1Q, which represents the commonly used value of 0x8100. The second is vMAN, which represents the commonly used value of 0x88A8. If EtherType is not one of these two values, then it is a custom tunnel value, representing any value in the range of 0 to 65535.

Voice VLAN Commands

This section describes the commands you use for Voice VLAN. Voice VLAN enables switch ports to carry voice traffic with defined priority so as to enable separation of voice and data traffic coming onto the port. The benefits of using Voice VLAN is to ensure that the sound quality of an IP phone could be safeguarded from deteriorating when the data traffic on the port is high.

Also the inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network- attached clients cannot initiate a direct attack on voice components. QoS-based on IEEE 802.1P class of service (CoS) uses classification and scheduling to sent network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

voice vlan (Global Config)

Use this command to enable the Voice VLAN capability on the switch.

Default disabled

Format `voice vlan`

Mode Global Config

no voice vlan (Global Config)

Use this command to disable the Voice VLAN capability on the switch.

Format	`no voice vlan`
Mode	Global Config

voice vlan (Interface Config)

Use this command to enable the Voice VLAN capability on the interface.

Default	disabled
Format	`voice vlan {<id> | dot1p <priority> | none | untagged}`
Mode	Interface Config

You can configure Voice VLAN in one of three different ways:

Parameter	Description
dot1p	Configure the IP phone to use 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. Valid <*priority*> range is 0 to 7.
none	Allow the IP phone to use its own configuration to send untagged voice traffic.
untagged	Configure the phone to send untagged voice traffic.

no voice vlan (Interface Config)

Use this command to disable the Voice VLAN capability on the interface.

Format	`no voice vlan`
Mode	Interface Config

voice vlan data priority

Use this command to either trust or untrust the data traffic arriving on the Voice VLAN port.

Default	trust
Format	`voice vlan data priority {untrust	trust}`
Mode	Interface Config

show voice vlan

Format	`show voice vlan [interface {<unit/slot/port>	all}]`
Mode	Privileged EXEC

When the **`interface`** parameter is not specified, only the global mode of the Voice VLAN is displayed.

Term	Definition
Administrative Mode	The Global Voice VLAN mode.

When the **`interface`** is specified:

Term	Definition
Voice VLAN Interface Mode	The admin mode of the Voice VLAN on the interface.
Voice VLAN ID	The Voice VLAN ID
Voice VLAN Priority	The do1p priority for the Voice VLAN on the port.
Voice VLAN Untagged	The tagging option for the Voice VLAN traffic.
Voice VLAN CoS Override	The Override option for the voice traffic arriving on the port.
Voice VLAN Status	The operational status of Voice VLAN on the port.

Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning, which allows you to prioritize ports.

vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the priority is 0-7. Any subsequent per port configuration will override this configuration setting.

Format	`vlan port priority all <`*`priority`*`>`
Mode	Global Config

vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the priority is 0–7.

Default	0
Format	`vlan priority <`*`priority`*`>`
Mode	Interface Config

Protected Ports Commands

This section describes commands you use to configure and view protected ports on a switch. Protected ports do not forward traffic to each other, even if they are on the same VLAN. However, protected ports can forward traffic to all unprotected ports in their group. Unprotected ports can forward traffic to both protected and unprotected ports. Ports are unprotected by default.

If an interface is configured as a protected port, and you add that interface to a Port Channel or Link Aggregation Group (LAG), the protected port status becomes operationally disabled on the interface, and the interface follows the configuration of the LAG port. However, the protected port configuration for the interface remains unchanged. Once the interface is no longer a member of a LAG, the current configuration for that interface automatically becomes effective.

switchport protected (Global Config)

Use this command to create a protected port group. The `<groupid>` parameter identifies the set of protected ports. Use the `name <name>` pair to assign a name to the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.

> ➡ **Note:** Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Format	`switchport protected <groupid> name <name>`
Mode	Global Config

no switchport protected (Global Config)

Use this command to remove a protected port group. The `groupid` parameter identifies the set of protected ports. Use the **name** keyword to remove the name from the group.

Format	`NO switchport protected <groupid> name`
Mode	Global Config

switchport protected (Interface Config)

Use this command to add an interface to a protected port group. The `<groupid>` parameter identifies the set of protected ports to which this interface is assigned. You can only configure an interface as protected in one group.

> ➡ **Note:** Port protection occurs within a single switch. Protected port configuration does not affect traffic between ports on two different switches. No traffic forwarding is possible between two protected ports.

Default	unprotected

Format	`switchport protected <groupid>`
Mode	Interface Config

no switchport protected (Interface Config)

Use this command to configure a port as unprotected. The *`groupid`* parameter identifies the set of protected ports to which this interface is assigned.

Format	`no switchport protected <groupid>`
Mode	Interface Config

show switchport protected

This command displays the status of all the interfaces, including protected and unprotected interfaces.

Format	`show switchport protected <groupid>`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Group ID	The number that identifies the protected port group.
Name	An optional name of the protected port group. The name can be up to 32 alphanumeric characters long, including blanks. The default is blank.
List of Physical Ports	List of ports, which are configured as protected for the group identified with <groupid>. If no port is configured as protected for this group, this field is blank.

show interfaces switchport

This command displays the status of the interface (protected/unprotected) under the groupid.

Format	`show interfaces switchport <unit/slot/port> <groupid>`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Name	A string associated with this group as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.
Protected port	Indicates whether the interface is protected or not. It shows TRUE or FALSE. If the group is a multiple groups then it shows TRUE in Group *<groupid>.*

Private Group Commands

This section describes commands used to configure private group and view private group configuration information.

Private group can be used to create a group of ports that can or can not share traffic to each others in the same VLAN group. The main application is to isolate a group of users from another without using VLAN.

switchport private-group

This command is used to assign one port or a range of ports to private group <privategroup-name> (or <private-group-id>).

The ingress traffic from a port in private group can be forwarded to other ports either in the same private group or anyone in the same VLAN that are not in a private group.

By default, a port does not belong to any private group. A port cannot be in more than one private group. An error message should return when that occurred. To change a port's private group, first the port must be removed from its private group.

Default	port not associated with any group.
Format	`switchport private-group [<privategroup-name>|<privategroup-id>]`
Mode	Interface Config

no switchport private group

This command is used to remove the specified port from the given private group.

Format	`no switchport private-group [<privategroup-name>|<privategroup-id>]`
Mode	Interface Config

private-group name

This command is used to create a private group with name <private-group-name>. The name string can be up to 24 bytes of non-blank characters. The total number of private groups is 192 such that the valid range for the ID is <1-192>.

The <private-group-id> field is optional. If not specified, a group id not used will be assigned automatically.

The mode can be either “isolated” or “community”. When in “isolated” mode, the member port in the group cannot forward its egress traffic to any other members in the same group. By default, the mode is “community” mode that each member port can forward traffic to other members in the same group, but not to members in other groups.

Format	`{<privategroup-name> mode [community|isolated]|<groupid>}`
Mode	Global Config

no private-group name

This command is used to remove the specified private group.

Format	`private-group name <privategroup-name>`
Mode	Global Config

show private-group

This command displays the private groups' information.

Format	`show private-groupname [<private-group-name>|<private-group-id>|port <unit/slot/port>]`
Mode	Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Port VLANID	The VLAN ID associated with the port.
Private Group ID	Total number of private groups is 192.
Private Group Name	The name string can be up to 24 bytes of non-blank characters
Private Group	The mode can be either “isolated” or “community”.

GARP Commands

This section describes the commands you use to configure Generic Attribute Registration Protocol (GARP) and view GARP status. The commands in this section affect both GARP VLAN Registration Protocol (GVRP) and Garp Multicast Registration Protocol (GMRP). GARP is a protocol that allows client stations to register with the switch for membership in VLANS (by using GVMP) or multicast groups (by using GVMP).

set garp timer join

This command sets the GVRP join time for one port (Interface Config mode) or all (Global Config mode) and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value 20 centiseconds is 0.2 seconds.

Default	20
Format	`set garp timer join <`*`10-100`*`>`
Mode	• Interface Config • Global Config

no set garp timer join

This command sets the GVRP join time (for one or all ports and per GARP) to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer join`
Mode	• Interface Config • Global Config

set garp timer leave

This command sets the GVRP leave time for one port (Interface Config mode) or all ports (Global Config mode) and only has an effect when GVRP is enabled. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. The leave time is 20 to 600 (centiseconds). The value 60 centiseconds is 0.6 seconds.

Default	60
Format	`set garp timer leave <`*`20-600`*`>`
Mode	• Interface Config • Global Config

no set garp timer leave

This command sets the GVRP leave time on all ports or a single port to the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leave`
Mode	• Interface Config • Global Config

set garp timer leaveall

This command sets how frequently Leave All PDUs are generated. A Leave All PDU indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from 200 to 6000 (centiseconds). The value 1000 centiseconds is 10 seconds. You can use this command on all ports (Global Config mode) or a single port (Interface Config mode), and it only has an effect only when GVRP is enabled.

Default	1000
Format	`set garp timer leaveall` *<200-6000>*
Mode	• Interface Config • Global Config

no set garp timer leaveall

This command sets how frequently Leave All PDUs are generated the default and only has an effect when GVRP is enabled.

Format	`no set garp timer leaveall`
Mode	• Interface Config • Global Config

show garp

This command displays GARP information.

Format	`show garp`
Mode	• Privileged EXEC • User EXEC

Term	Definition
GMRP Admin Mode	The administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.
GVRP Admin Mode	The administrative mode of GARP VLAN Registration Protocol (GVRP) for the system.

GVRP Commands

This section describes the commands you use to configure and view GARP VLAN Registration Protocol (GVRP) information. GVRP-enabled switches exchange VLAN configuration information, which allows GVRP to provide dynamic VLAN creation on trunk ports and automatic VLAN pruning.

➡ **Note:** If GVRP is disabled, the system does not forward GVRP messages.

set gvrp adminmode

This command enables GVRP on the system.

Default	disabled
Format	`set gvrp adminmode`
Mode	Privileged EXEC

no set gvrp adminmode

This command disables GVRP.

Format	`no set gvrp adminmode`
Mode	Privileged EXEC

set gvrp interfacemode

This command enables GVRP on a single port (Interface Config mode) or all ports (Global Config mode).

Default	disabled
Format	`set gvrp interfacemode`
Mode	• Interface Config • Global Config

no set gvrp interfacemode

This command disables GVRP on a single port (Interface Config mode) or all ports (Global Config mode). If GVRP is disabled, Join Time, Leave Time and Leave All Time have no effect.

Format	`no set gvrp interfacemode`
Mode	• Interface Config • Global Config

show gvrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gvrp configuration {<unit/slot/port> | all}`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is one centisecond (0.01 seconds).

Term	Definition
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GVMRP Mode	The GVRP administrative mode for the port, which is enabled or disabled (default). If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

GMRP Commands

This section describes the commands you use to configure and view GARP Multicast Registration Protocol (GMRP) information. Like IGMP snooping, GMRP helps control the flooding of multicast packets.GMRP-enabled switches dynamically register and de-register group membership information with the MAC networking devices attached to the same segment. GMRP also allows group membership information to propagate across all networking devices in the bridged LAN that support Extended Filtering Services.

Note: If GMRP is disabled, the system does not forward GMRP messages.

set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system.

Default	disabled
Format	`set gmrp adminmode`
Mode	Privileged EXEC

no set gmrp adminmode

This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format	`no set gmrp adminmode`
Mode	Privileged EXEC

set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a single interface (Interface Config mode) or all interfaces (Global Config mode). If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled on that interface. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Default	disabled
Format	`set gmrp interfacemode`
Mode	• Interface Config • Global Config

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a single interface or all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a port-channel (LAG), GARP functionality is disabled. GARP functionality is subsequently re-enabled if routing is disabled and port-channel (LAG) membership is removed from an interface that has GARP enabled.

Format	`no set gmrp interfacemode`
Mode	• Interface Config • Global Config

show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format	`show gmrp configuration {<unit/slot/port> | all}`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	The unit/slot/port of the interface that this row in the table describes.
Join Timer	The interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-port, per-GARP participant basis. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). The finest granularity of specification is 1 centisecond (0.01 seconds).
Leave Timer	The period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
LeaveAll Timer	This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Port GMRP Mode	The GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect.

show mac-address-table gmrp

This command displays the GMRP entries in the Multicast Forwarding Database (MFDB) table.

Format	`show mac-address-table gmrp`
Mode	Privileged EXEC

Term	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Port-Based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (802.1x). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

Format	`clear dot1x statistics` *{<unit/slot/port> | all}*
Mode	Privileged EXEC

clear radius statistics

This command is used to clear all RADIUS statistics.

Format	`clear radius statistics`
Mode	Privileged EXEC

dot1x guest-vlan

This command configures VLAN as guest vlan on a per port basis. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Default	disabled
Format	`dot1x guest-vlan <`*`vlan-id`*`>`
Mode	Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Default	disabled
Format	`no dot1x guest-vlan`
Mode	Interface Config

dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is “auto” or “mac-based”. If the control mode is not 'auto' or “mac-based”, an error will be returned.

Format	`dot1x initialize <`*`unit/slot/port`*`>`
Mode	Privileged EXEC

dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The `<count>` value must be in the range 1 - 10.

Default	2

Format	`dot1x max-req <count>`
Mode	Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format	`no dot1x max-req`
Mode	Interface Config

dot1x max-users

Use this command to set the maximum number of clients supported on the port when MAC-based dot1x authentication is enabled on the port. The maximum users supported per port is dependent on the product. The `<count>` value is in the range 1 - 16.

Default	16
Format	`dot1x max-users <count>`
Mode	Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format	`no dot1x max-req`
Mode	Interface Config

dot1x port-control

This command sets the authentication mode to use on the specified port. Select *`force-unauthorized`* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *`force-authorized`* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *`auto`* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control` *`{force-unauthorized`* `|` *`force-authorized`* `|` *`auto`* `|` *`mac-based}`*
Mode	Interface Config

no dot1x port-control

This command sets the 802.1x port control mode on the specified port to the default value.

Format	`no dot1x port-control`
Mode	Interface Config

dot1x port-control all

This command sets the authentication mode to use on all ports. Select *`force-unauthorized`* to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select *`force-authorized`* to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select *`auto`* to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the `mac-based` option is specified, then MAC-based dot1x authentication is enabled on the port.

Default	auto
Format	`dot1x port-control all` *`{force-unauthorized`* `|` *`force-authorized`* `|` *`auto`* `|` *`mac-based}`*
Mode	Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format	`no dot1x port-control all`
Mode	Global Config

dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is “auto” or “mac-based”. If the control mode is not “auto” or “mac-based”, an error will be returned.

Format	`dot1x re-authenticate` *`<unit/slot/port>`*
Mode	Privileged EXEC

dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default	disabled
Format	`dot1x re-authentication`
Mode	Interface Config

no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format	`no dot1x re-authentication`
Mode	Interface Config

dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default	disabled
Format	`dot1x system-auth-control`
Mode	Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format	`no dot1x system-auth-control`
Mode	Global Config

dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Tokens	Definition
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default	• guest-vlan-period: 90 seconds • reauth-period: 3600 seconds • quiet-period: 60 seconds • tx-period: 30 seconds • supp-timeout: 30 seconds • server-timeout: 30 seconds
Format	`dot1x timeout` *`{{guest-vlan-period <seconds>} |{reauth-period <seconds>}	{quiet-period <seconds>}	{tx-period <seconds>}	{supp-timeout <seconds>}	{server-timeout <seconds>}}`*
Mode	Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format	`no dot1x timeout` *`{guest-vlan-period	reauth-period	quiet-period	tx-period	supp-timeout	server-timeout}`*
Mode	Interface Config

dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with that port. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093 for 7000 series). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default	0
Format	`dot1x unauthenticated-vlan <`*`vlan id`*`>`
Mode	Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format	`no dot1x unauthenticated-vlan`
Mode	Interface Config

dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The *`<user>`* parameter must be a configured user.

Format	`dot1x user` *`<user> {<unit/slot/port>	all}`*
Mode	Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format	`no dot1x user` *`<user> {<unit/slot/port>	all}`*
Mode	Global Config

clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format	*`clear dot1x authentication-history [unit/slot/port]`*
Mode	Global Config

dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS assigned VLAN does not exist in the switch.

Format	*`dot1x dynamic-vlan enable`*
Mode	Global Config
Default	Disabled

no dot1x dynamic-vlan enable

Use this command to disable the switch from creating VLANs dynamically when a RADIUS assigned VLAN does not exist in the switch.

Format	*`no dot1x dynamic-vlan enable`*
Mode	Global Config

dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Format	*`dot1x system-auth-control monitor`*
Mode	Global Config
Default	Disabled

no dot1x system-auth-control monitor

Use this command to disable the 802.1X monitor on the switch.

Format	*`no dot1x system-auth-control monitor`*
Mode	Global Config

show dot1x authentication-history

This command displays 802.1X authentication events and information during successful and unsuccessful Dot1x authentication process for all interfaces or the specified interface. Use the optional keywords to display only failure authentication events in summary or in detail.

Format	*show dot1x authentication-history {unit/slot/port | all} [failedauth-only] [detail]*
Mode	Privileged EXEC

Term	Definition
Time Stamp	The exact time at which the event occurs..
Interface	Physical Port on which the event occurs.
Mac-Address	The supplicant/client MAC address..
VLAN assigned	The VLAN assigned to the client/port on authentication..
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Montior Mode VLAN ID.
Auth Status	The authentication status.
Reason	The actual reason behind the successful or failed authentication.

show authentication methods

This command displays information about the authentication methods.

Format	`show authentication methods`
Mode	Privileged EXEC

The following is an example of this command:

```
Login Authentication Method Lists
________________________________
Console_Default: None
Network_Default:Local
Enable Authentication Lists
_____________________
Console_Default: Enable None
Network_Default:Enable
Line Login Method List Enable Method Lists
```

```
Console Console_Default Console_Default
Telnet Network_Default Network_Default
SSH Network_Default Network_Default
http : Local
https : Local
dot1x :
```

show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format	`show dot1x` *`[{summary {<unit/slot/port>	all}	detail <unit/slot/port>	statistics <unit/slot/port>]`*
Mode	Privileged EXEC

If you do not use the optional parameters *`<unit/slot/port>`* or *`<vlanid>`*, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Term	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.
VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

If you use the optional parameter *`summary {<unit/slot/port> | all}`*, the dot1x configuration for the specified port or all ports are displayed.

Term	Definition
Interface	The interface whose configuration is displayed.

Term	Definition
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether re-authentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

If you use the optional parameter '**`detail`** *`<unit/slot/port>`*', the detailed dot1x configuration for the specified port is displayed.

Term	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | force-authorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.

Term	Definition
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
VLAN Id	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN Idfield has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is ‘Not Assigned’, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are ‘True” or “False”.
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MAC-based.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control mode is not MAC-based.

The `show dot1x detail <unit/slot/port>` command will display the following MAC-based dot1x fields if the port-control mode for that specific port is MAC-based. For each client authenticated on the port, the `show dot1x detail <unit/slot/port>` command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Term	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter **`statistics`** *`<unit/slot/port>`*, the following dot1x statistics for the specified port appear.

Term	Definition
Port	The interface whose statistics are displayed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.

Term	Definition
EAP Response/ Id Frames Received	The number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

show dot1x clients

This command displays 802.1x client information.This command also displays information about the number of clients that are authenticated using Monitor mode and using 802.1X.

Format	`show dot1x clients {<unit/slot/port>	all}`
Mode	Privileged EXEC

Term	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.

Term	Definition
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supplicant MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.
Filter ID	Identifies the Filter ID returned by the RADIUS server when the client was authenticated. This is a configured DiffServ policy name on the switch.
VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the PVID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

show dot1x users

This command displays 802.1x port security user information for locally configured users.

Format	`show dot1x users` *`<unit/slot/port>`*
Mode	Privileged EXEC

Term	Definition
Users	Users configured locally to have access to the specified port.

Storm-Control Commands

This section describes commands you use to configure storm-control and view storm-control configuration information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

The 7000 series provides broadcast, multicast, and unicast story recovery for individual interfaces. Unicast Storm-Control protects against traffic whose MAC addresses are not known by the system. For broadcast, multicast, and unicast storm-control, if the rate of traffic ingressing on an interface increases beyond the configured threshold for that type, the traffic is dropped.

To configure storm-control, you will enable the feature for all interfaces or for individual interfaces, and you will set the threshold (storm-control level) beyond which the broadcast, multicast, or unicast traffic will be dropped. The Storm-Control feature allows you to limit the rate of specific types of packets through the switch on a per-port, per-type, basis.

Configuring a storm-control level also enables that form of storm-control. Disabling a storm-control level (using the “no” version of the command) sets the storm-control level back to the default value and disables that form of storm-control. Using the “no” version of the “storm-control” command (not stating a “level”) disables that form of storm-control but maintains the configured “level” (to be active the next time that form of storm-control is enabled.)

Note: The actual rate of ingress traffic required to activate storm-control is based on the size of incoming packets and the hard-coded average packet size of 512 bytes - used to calculate a packet-per-second (pps) rate - as the forwarding-plane requires pps versus an absolute rate kbps. For example, if the configured limit is 10%, this is converted to ~25000 pps, and this pps limit is set in forwarding plane (hardware). You get the approximate desired output when 512bytes packets are used.

storm-control broadcast

Use this command to enable broadcast storm recovery mode for a specific interface. If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	enabled
Format	`storm-control broadcast`
Mode	Interface Config

no storm-control broadcast

Use this command to disable broadcast storm recovery mode for a specific interface.

Format	`no storm-control broadcast`
Mode	Interface Config

storm-control broadcast level

Use this command to configure the broadcast storm recovery threshold for an interface as a percentage of link speed and enable broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	5
Format	`storm-control broadcast level` *<0-100>*
Mode	Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	`no storm-control broadcast level`
Mode	Interface Config

storm-control broadcast rate

Use this command to configure the broadcast storm recovery threshold for an interface in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0
Format	`storm-control broadcast rate <0-14880000>`
Mode	Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for an interface and disables broadcast storm recovery.

Format	`no storm-control broadcast rate`
Mode	Interface Config

storm-control broadcast (Global)

This command enables broadcast storm recovery mode for all interfaces. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control broadcast`
Mode	Global Config

no storm-control broadcast

This command disables broadcast storm recovery mode for all interfaces.

Format	`no storm-control broadcast`
Mode	Global Config

storm-control broadcast level (Global)

This command configures the broadcast storm recovery threshold for all interfaces as a percentage of link speed and enables broadcast storm recovery. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.This command also enables broadcast storm recovery mode for all interfaces.

Default	5
Format	`storm-control broadcast level` <*0-100*>
Mode	Global Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	`no storm-control broadcast level`
Mode	Global Config

storm-control broadcast rate (Global)

Use this command to configure the broadcast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Default	0

Format	`storm-control broadcast rate <`*`0-14880000`*`>`
Mode	Global Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	`no storm-control broadcast rate`
Mode	Global Config

storm-control multicast

This command enables multicast storm recovery mode for an interface. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control multicast`
Mode	Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for an interface.

Format	`no storm-control multicast`
Mode	Interface Config

storm-control multicast level

This command configures the multicast storm recovery threshold for an interface as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	`storm-control multicast level <0-100>`
Mode	Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	`no storm-control multicast level <0-100>`
Mode	Interface Config

storm-control multicast rate

Use this command to configure the multicast storm recovery threshold for an interface in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control multicast rate <0-14880000>`
Mode	Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	`no storm-control multicast rate`
Mode	Interface Config

storm-control multicast (Global)

This command enables multicast storm recovery mode for all interfaces. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control multicast`
Mode	Global Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces.

Format	`no storm-control multicast`
Mode	Global Config

storm-control multicast level (Global)

This command configures the multicast storm recovery threshold for all interfaces as a percentage of link speed and enables multicast storm recovery mode. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Default	5
Format	`storm-control multicast level <0-100>`
Mode	Global Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces and disables multicast storm recovery.

Format	`no storm-control multicast level`
Mode	Global Config

storm-control multicast rate (Global)

Use this command to configure the multicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control multicast rate <`*`0-14880000`*`>`
Mode	Global Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces and disables broadcast storm recovery.

Format	`no storm-control broadcast rate`
Mode	Global Config

storm-control unicast

This command enables unicast storm recovery mode for an interface. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control unicast`
Mode	Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for an interface.

Format	`no storm-control unicast`
Mode	Interface Config

storm-control unicast level

This command configures the unicast storm recovery threshold for an interface as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.This command also enables unicast storm recovery mode for an interface.

Default	5
Format	`storm-control unicast level <`*`0-100`*`>`
Mode	Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format	`no storm-control unicast level`
Mode	Interface Config

storm-control unicast rate

Use this command to configure the unicast storm recovery threshold for an interface in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control unicast rate <0-14880000>`
Mode	Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for an interface and disables unicast storm recovery.

Format	`no storm-control unicast rate`
Mode	Interface Config

storm-control unicast (Global)

This command enables unicast storm recovery mode for all interfaces. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	disabled
Format	`storm-control unicast`
Mode	Global Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces.

Format	`no storm-control unicast`
Mode	Global Config

storm-control unicast level (Global)

This command configures the unicast storm recovery threshold for all interfaces as a percentage of link speed, and enables unicast storm recovery. If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Default	5
Format	`storm-control unicast level <`*`0-100`*`>`
Mode	Global Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value and disables unicast storm recovery for all interfaces.

Format	`no storm-control unicast level`
Mode	Global Config

storm-control unicast rate (Global)

Use this command to configure the unicast storm recovery threshold for all interfaces in packets per second. If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of unicast traffic is limited to the configured threshold.

Default	0
Format	`storm-control unicast rate <`*`0-14880000`*`>`
Mode	Global Config

no storm-control unicast rate

This command sets the multicast storm recovery threshold to the default value for an interface and disables multicast storm recovery.

Format	`no storm-control unicast rate`
Mode	Global Config

storm-control flowcontrol

This command enables 802.3x flow control for the switch and only applies to full-duplex mode ports.

➡ **Note:** 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss.

Default	disabled
Format	`storm-control flowcontrol`
Mode	Global Config

no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

➡ **Note:** This command only applies to full-duplex mode ports.

Format	`no storm-control flowcontrol`
Mode	Global Config

show storm-control

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Control Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.
- **Broadcast Storm Control Level** The broadcast storm control level. The factory default is 5%.
- **Multicast Storm Control Mode** may be enabled or disabled. The factory default is disabled.
- **Multicast Storm Control Level** The multicast storm control level. The factory default is 5%.
- **Unicast Storm Control Mode** may be enabled or disabled. The factory default is disabled.
- **Unicast Storm Control Level** The unicast storm control level. The factory default is 5%.

Use the **`all`** keyword to display the per-port configuration parameters for all interfaces, or specify the *`unit/slot/port`* to display information about a specific interface.

Format	`show storm-control` *`[all	<unit/slot/port>]`*
Mode	Privileged EXEC

Term	Definition
Bcast Mode	Shows whether the broadcast storm control mode is enabled or disabled. The factory default is disabled.
Bcast Level	The broadcast storm control level.
Mcast Mode	Shows whether the multicast storm control mode is enabled or disabled.
Mcast Level	The multicast storm control level.
Ucast Mode	Shows whether the Unknown Unicast or DLF (Destination Lookup Failure) storm control mode is enabled or disabled.
Ucast Level	The Unknown Unicast or DLF (Destination Lookup Failure) storm control level.

Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address.Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols.) A static port-channel interface does not require a partner system to be able to aggregate its member ports.

> **Note:** If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

addport

This command adds one port to the port-channel (LAG). The interface is a logical unit/slot/port number or a group ID of a configured port-channel.

> **Note:** Before adding a port to a port-channel, set the physical mode of the port. For more information, see "speed" on page 3-7

Format	`addport {<logical unit/slot/port>|<lag-group-id>}`
Mode	Interface Config

deleteport (Interface Config)

This command deletes the port from the port-channel (LAG). The interface is a logical unit/slot/port number or a group ID of a configured port-channel.

Format	`deleteport {<logical unit/slot/port>|<lag-group-id>}`
Mode	Interface Config

deleteport (Global Config)

This command deletes all configured ports from the port-channel (LAG). The interface is a logical unit/slot/port number of a configured port-channel. To clear the port channels, see "clear port-channel" on page 6-27.

Format	`deleteport <logical unit/slot/port> all`
Mode	Global Config

lacp admin key

Use this command to configure the administrative value of the key for the port-channel. The value range of <*key*> is 0 to 65535.

Default	0x8000
Format	`lacp admin key <key>`
Mode	Interface Config

Note: This command is only applicable to port-channel interfaces.

no lacp admin key

Use this command to configure the default administrative value of the key for the port-channel.

Format	`no lacp admin key`
Mode	Interface Config

lacp collector max-delay

Use this command to configure the port-channel collector max delay. The valid range of <*delay*> is 0-65535.

Default	0x8000
Format	`lacp collector max-delay <delay>`
Mode	Interface Config

Note: This command is only applicable to port-channel interfaces.

no lacp collector max delay

Use this command to configure the default port-channel collector max delay.

Format	`no lacp collector max-delay`
Mode	Interface Config

lacp actor admin

Use this command to configure the LACP actor admin parameters.

lacp actor admin key

Use this command to configure the administrative value of the LACP actor admin key. The valid range for <*key*> is 0-65535.

Default	Internal Interface Number of this Physical Port
Format	`lacp actor admin key <key>`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin key

Use this command to configure the default administrative value of the key.

Format	`no lacp actor admin key`
Mode	Interface Config

lacp actor admin state individual

Use this command to set LACP actor admin state to individual.

Format	`lacp actor admin state individual`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state individual

Use this command to set the LACP actor admin state to aggregation.

Format	`no lacp actor admin state individual`
Mode	Interface Config

lacp actor admin state longtimeout

Use this command to set LACP actor admin state to longtimeout.

Format	`lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout.

Format	`no lacp actor admin state longtimeout`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

lacp actor admin state passive

Use this command to set the LACP actor admin state to passive.

Format	`lacp actor admin state passive`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active.

Format	`no lacp actor admin state passive`
Mode	Interface Config

lacp actor port priority

Use this command to configure the priority value assigned to the Aggregation Port. The valid range for <`priority`> is 0 to 255.

Default	0x80
Format	`lacp actor port priority <priority>`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port.

Format	`no lacp actor port priority`
Mode	Interface Config

lacp actor system priority

Use this command to configure the priority value associated with the LACP Actor's SystemID. The range for <`priority`> is 0 to 65535.

Default	32768
Format	`lacp actor system priority <priority>`
Mode	Interface Config

➡ **Note:** This command is only applicable to physical interfaces.

no lacp actor system priority

Use this command to configure the priority value associated with the Actor's SystemID.

Format	`no lacp actor system priority`
Mode	Interface Config

lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner. The valid range for <*key*> is 0 to 65535.

Default	0x0
Format	`lacp partner admin key`
Mode	Interface Config

➡ **Note:** This command is only applicable to physical interfaces.

no lacp partner admin key

Use this command to configure the administrative value of the Key for the protocol partner.

Format	`no lacp partner admin key <key>`
Mode	Interface Config

lacp partner admin state individual

Use this command to set LACP partner admin state to individual.

Format	`lacp partner admin state individual`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state individual

Use this command to set the LACP partner admin state to aggregation.

Format	`no lacp partner admin state individual`
Mode	Interface Config

lacp partner admin state longtimeout

Use this command to set LACP partner admin state to longtimeout.

Format	`lacp partner admin state longtimeout`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state longtimeout

Use this command to set the LACP partner admin state to short timeout.

Format	`no lacp partner admin state longtimeout`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

lacp partner admin state passive

Use this command to set the LACP partner admin state to passive.

Format	`lacp partner admin state passive`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner admin state passive

Use this command to set the LACP partner admin state to active.

Format	`no lacp partner admin state passive`
Mode	Interface Config

lacp partner port id

Use this command to configure the LACP partner port id. The valid range for <*port-id*> is 0 to 65535.

Default	0x80
Format	`lacp partner portid <port-id>`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner port id

Use this command to set the LACP partner port id to the default.

Format	`no lacp partner portid`
Mode	Interface Config

lacp partner port priority

Use this command to configure the LACP partner port priority. The valid range for <*priority*> is 0 to 255.

Default	0x0
Format	`lacp partner port priority <priority>`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner port priority

Use this command to configure the default LACP partner port priority.

Format	`no lacp partner port priority`
Mode	Interface Config

lacp partner system id

Use this command to configure the 6-octet MAC Address value representing the administrative value of the Aggregation Port’s protocol Partner’s System ID. The valid range of <*`system-id`*> is 00:00:00:00:00:00 - FF:FF:FF:FF:FF.

Default	00:00:00:00:00:00
Format	`lacp partner system id <`*`system-id`*`>`
Mode	Interface Config

➡ **Note:** This command is only applicable to physical interfaces.

no lacp partner system id

Use this command to configure the default value representing the administrative value of the Aggregation Port’s protocol Partner’s System ID.

Format	`no lacp partner system id`
Mode	Interface Config

lacp partner system priority

Use this command to configure the administrative value of the priority associated with the Partner’s System ID. The valid range for <*priority*> is 0 to 65535.

Default	0x0
Format	`lacp partner system priority <priority>`
Mode	Interface Config

Note: This command is only applicable to physical interfaces.

no lacp partner system priority

Use this command to configure the default administrative value of priority associated with the Partner’s System ID.

Format	`no lacp partner system priority`
Mode	Interface Config

port-channel static

This command enables the static mode on a port-channel (LAG) interface. By default the static mode for a new port-channel is disabled, which means the port-channel is dynamic. However if the maximum number of allowable dynamic port-channels are already present in the system, the static mode for a new port-channel enabled, which means the port-channel is static.You can only use this command on port-channel interfaces.

Default	disabled
Format	`port-channel static`
Mode	Interface Config

no port-channel static

This command sets the static mode on a particular port-channel (LAG) interface to the default value. This command will be executed only for interfaces of type port-channel (LAG).

Format	`no port-channel static`
Mode	Interface Config

port lacpmode

This command enables Link Aggregation Control Protocol (LACP) on a port.

Default	enabled
Format	`port lacpmode`
Mode	Interface Config

no port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format	`no port lacpmode`
Mode	Interface Config

port lacpmode enable all

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format	`port lacpmode enable all`
Mode	Global Config

no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format	`no port lacpmode enable all`
Mode	Global Config

port lacptimeout (Interface Config)

This command sets the timeout on a physical interface of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default	long
Format	`port lacptimeout` *`{actor	partner} {long	short}`*
Mode	Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (**actor** or **partner**).

Format	`no port lacptimeout` *`{actor	partner}`*
Mode	Interface Config

port lacptimeout (Global Config)

This command sets the timeout for all interfaces of a particular device type (**actor** or **partner**) to either **long** or **short** timeout.

Default	long
Format	`port lacptimeout` *`{actor	partner} {long	short}`*
Mode	Global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (**actor** or **partner**) back to their default values.

Format	`no port lacptimeout {actor	partner}`
Mode	Global Config

port-channel adminmode

This command enables a port-channel (LAG). This command sets every configured port-channel with the same administrative mode setting.

Format	`port-channel adminmode all`
Mode	Global Config

no port-channel adminmode

This command disables a port-channel (LAG). This command clears every configured port-channel with the same administrative mode setting.

Format	`no port-channel adminmode [all]`
Mode	Global Config

port-channel linktrap

This command enables link trap notifications for the port-channel (LAG). The interface is a logical unit/slot/port for a configured port-channel. The option **`all`** enables link trap notifications for all the configured port-channels.

Default	enabled
Format	`port-channel linktrap {<logical unit/slot/port>	all}`
Mode	Global Config

no port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option **`all`** disables link trap notifications for all the configured port-channels.

Format	`no port-channel linktrap {<logical unit/slot/port> | all}`
Mode	Global Config

port-channel load-balance

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port-channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device. The XSM7224S also supports enhanced hashing mode, which has the following advantages:

- MODULO-N (where N is the number of active link members in a LAG) operation based on the number of ports in the LAG
- Packet attributes selection based on the packet type: For L2 packets, source and destination MAC address are used for hash computation. For L3 packets, source IP, destination IP address, TCP/UDP ports are used.
- Non-Unicast traffic and unicast traffic is hashed using a common hash algorithm
- Excellent load balancing performance

.

Default	3
Format	`port-channel load-balance { 1 | 2 | 3 | 4 | 5 | 6 | 7} {<unit/slot/port> |<all>}`
Mode	Interface Config Global Config

Term	Definition
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet

Term	Definition
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
7	Enhanced Hashing Mode
<unit/slot/ port>| all	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel. "All" applies the command to all currently configured port-channels.

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format	`no port-channel load-balance {<unit/slot/port>	<all>}`
Mode	Interface Config Global Config

Term	Definition
<unit/slot/ port>| all	Global Config Mode only: The interface is a logical unit/slot/port number of a configured port-channel. "All" applies the command to all currently configured port-channels.

port-channel name

This command defines a name for the port-channel (LAG). The interface is a logical unit/slot/port for a configured port-channel, and `<name>` is an alphanumeric string up to 15 characters.

Format	`port-channel name {<logical unit/slot/port>	all	<name>}`
Mode	Global Config

port-channel system priority

Use this command to configure port-channel system priority. The valid range of <priority> is 0-65535.

Default	0x8000
Format	`port-channel system priority <`*`priority`*`>`
Mode	Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format	`no port-channel system priority`
Mode	Global Config

show lacp actor

Use this command to display LACP actor attributes.

Format	`show lacp actor {<`*`unit/slot/port`*`>|all}`
Mode	Global Config

The following output parameters are displayed.

Parameter	Description
System Priority	The system priority assigned to the Aggregation Port.
Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

show lacp partner

Use this command to display LACP partner attributes.

Format	`show lacp partner {<unit/slot/port>|all}`
Mode	Privileged EXEC

The following output parameters are displayed.

Parameter	Description
System Priority	The administrative value of priority associated with the Partner's System ID.
System ID	The value representing the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the port priority for the protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

show port-channel brief

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces.

Format	`show port-channel brief`
Mode	• Privileged EXEC • User EXEC

For each port-channel the following information is displayed:

Term	Definition
Logical Interface	The unit/slot/port of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.

Term	Definition
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays the static capability of all port-channels (LAGs) on the device as well as a summary of individual port-channels.

Format	`show port-channel`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Static Capability	This field displays whether or not the device has static capability enabled.

For each port-channel the following information is displayed:

Term	Definition
Name	This field displays the name of the port-channel.
Link-State	Shows whether the link is up or down.
Mbr Ports	This field lists the ports that are members of this port-channel, in *<unit/slot/port***>** notation.
Active Ports	The ports that are actively participating in the port-channel.

show port-channel

This command displays an overview of all port-channels (LAGs) on the switch.

Format	`show port-channel` *`{<logical unit/slot/port>	all}`*
Mode	• Privileged EXEC • User EXEC

Term	Definition
Logical Interface	Valid slot and port number separated by forward slashes.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** - The port-channel is statically maintained. • **Dynamic** - The port-channel is dynamically maintained.
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in unit/slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (**long** or **short**) for Device Type (**actor** or **partner**).
Port Speed	Speed of the port-channel port.
Ports Active	This field lists ports that are actively participating in the port-channel (LAG).
Load Balance Option	The load balance option associated with this LAG. See "port-channel load-balance" on page 3-110.

show port-channel system priority

Use this command to display the port-channel system priority.

Format	`show port-channel system priority`
Mode	Privileged EXEC

Port Mirroring

Port mirroring, which is also known as port monitoring, selects network traffic that you can analyze with a network analyzer, such as a SwitchProbe device or other Remote Monitoring (RMON) probe.

monitor session

This command configures a probe port and a monitored port for monitor session (port monitoring). Use the *`source interface <unit/slot/port>`* parameter to specify the interface to monitor. Use *`rx`* to monitor only ingress packets, or use *`tx`* to monitor only egress packets. If you do not specify an *`{rx | tx}`* option, the destination port monitors both ingress and egress packets. Use the *`destination interface <unit/slot/port>`* to specify the interface to receive the monitored traffic. Use the *`mode`* parameter to enabled the administrative mode of the session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format	`monitor session` *`<session-id> {source interface <unit/slot/port> [{rx	tx}]	destination interface <unit/slot/port>	mode}`*
Mode	Global Config

no monitor session

Use this command without optional parameters to remove the monitor session (port monitoring) designation from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs. Use the *`source interface <unit/slot/port>`* parameter or *`destination interface <unit/slot/port>`* to remove the specified interface from the port monitoring session. Use the *`mode`* parameter to disable the administrative mode of the session

> ➡ **Note:** Since the current version of 7000 series software only supports one session, if you do not supply optional parameters, the behavior of this command is similar to the behavior of the `no monitor` command.

Format	`no monitor session` *`<session-id> [{source interface <unit/slot/port>	destination interface <unit/slot/port>	mode}]`*
Mode	Global Config

no monitor

This command removes all the source ports and a destination port for the and restores the default value for mirroring session mode for all the configured sessions.

> **Note:** This is a stand-alone “no” command. This command does not have a “normal” form.

Default	enabled
Format	`no monitor`
Mode	Global Config

show monitor session

This command displays the Port monitoring information for a particular mirroring session.

> **Note:** The `<session-id>` parameter is an integer value used to identify the session. In the current version of the software, the `<session-id>` parameter is always one (1)

Format	`show monitor session <session-id>`
Mode	Privileged EXEC

Term	Definition
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Admin Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with <*session-id*>. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with `<session-id>`. If probe port is not set then this field is blank.
Mirrored Port	The port, which is configured as mirrored port (source port) for the session identified with `<session-id>`**.** If no source port is configured for the session then this field is blank.
Type	Direction in which source port configured for port mirroring.Types are tx for transmitted packets and rx for receiving packets.

Static MAC Filtering

The commands in this section describe how to configure static MAC filtering. Static MAC filtering allows you to configure destination ports for a static multicast MAC filter irrespective of the platform.

macfilter

This command adds a static MAC filter entry for the MAC address *<macaddr>* on the VLAN *<vlanid>*. The value of the *<macaddr>* parameter is a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF. The *<vlanid>* parameter must identify a valid VLAN.

The number of static mac filters supported on the system is different for MAC filters where source ports are configured and MAC filters where destination ports are configured.

- For unicast MAC address filters and multicast MAC address filters with source port lists, the maximum number of static MAC filters supported is 20.
- For multicast MAC address filters with destination ports configured, the maximum number of static filters supported is 256.

i.e. For current platforms, you can configure the following combinations:

- Unicast MAC and source port (max = 20)
- Multicast MAC and source port (max=20)
- Multicast MAC and destination port (only) (max=256)
- Multicast MAC and source ports and destination ports (max=20)

Format	`macfilter <macaddr> <vlanid>`
Mode	Global Config

no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address *<macaddr>* on the VLAN *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *<vlanid>* parameter must identify a valid VLAN.

Format	`no macfilter <macaddr> <vlanid>`
Mode	Global Config

macfilter adddest

Use this command to add the interface to the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

➡ **Note:** Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest <macaddr> <vlanid>`
Mode	Interface Config

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	`no macfilter adddest <macaddr> <vlanid>`
Mode	Interface Config

macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

➡	**Note:** Configuring a destination port list is only valid for multicast MAC addresses.

Format	`macfilter adddest all <macaddr> <vlanid>`
Mode	Global Config

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given *<macaddr>* and VLAN of *<vlanid>*. The *<macaddr>* parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	`no macfilter adddest all <macaddr> <vlanid>`
Mode	Global Config

macfilter addsrc

This command adds the interface to the source filter set for the MAC filter with the MAC address of <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	`macfilter addsrc <macaddr> <vlanid>`
Mode	Interface Config

no macfilter addsrc

This command removes a port from the source filter set for the MAC filter with the MAC address of *<macaddr>* and VLAN of *<vlanid>*. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	`no macfilter addsrc <macaddr> <vlanid>`
Mode	Interface Config

macfilter addsrc all

This command adds all interfaces to the source filter set for the MAC filter with the MAC address of *<macaddr>* and *<vlanid>*. You must specify the *<macaddr>* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6. The *<vlanid>* parameter must identify a valid VLAN.

Format	`macfilter addsrc all <macaddr> <vlanid>`
Mode	Global Config

no macfilter addsrc all

This command removes all interfaces to the source filter set for the MAC filter with the MAC address of *<macaddr>* and VLAN of *<vlanid>*. You must specify the *<macaddr>* parameter as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The *<vlanid>* parameter must identify a valid VLAN.

Format	`no macfilter addsrc all <macaddr> <vlanid>`
Mode	Global Config

show mac-address-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If you select <*all*>, all the Static MAC Filters in the system are displayed. If you supply a value for <*macaddr*>, you must also enter a value for <*vlanid*>, and the system displays Static MAC Filter information only for that MAC address and VLAN.

Format	`show mac-address-table static {<macaddr> <vlanid>	all}`
Mode	Privileged EXEC

Term	Definition
MAC Address	The MAC Address of the static MAC filter entry.
VLAN ID	The VLAN ID of the static MAC filter entry.
Source Port(s)	The source port filter set's slot and port(s).

Note: Only multicast address filters will have destination port lists.

show mac-address-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format	`show mac-address-table staticfiltering`
Mode	Privileged EXEC

Term	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. As the data is gleaned from the MFDB, the address will be a multicast address. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Term	Definition
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

DHCP Snooping Configuration Commands

This section describes commands you use to configure DHCP Snooping.

ip dhcp snooping

Use this command to enable DHCP Snooping globally.

Default	disabled
Format	`ip dhcp snooping`
Mode	Global Config

no ip dhcp snooping

Use this command to disable DHCP Snooping globally.

Format	`no ip dhcp snooping`
Mode	Global Config

ip dhcp snooping vlan

Use this command to enable DHCP Snooping on a list of comma-separated VLAN ranges.

Default	disabled
Format	`ip dhcp snooping vlan <vlan-list>`
Mode	Global Config

no ip dhcp snooping vlan

Use this command to disable DHCP Snooping on VLANs.

Format	`no ip dhcp snooping vlan <`*`vlan-list`*`>`
Mode	Global Config

ip dhcp snooping verify mac-address

Use this command to enable verification of the source MAC address with the client hardware address in the received DCHP message.

Default	enabled
Format	`ip dhcp snooping verify mac-address`
Mode	Global Config

no ip dhcp snooping verify mac-address

Use this command to disable verification of the source MAC address with the client hardware address.

Format	`no ip dhcp snooping verify mac-address`
Mode	Global Config

ip dhcp snooping database

Use this command to configure the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

Default	local
Format	`ip dhcp snooping database {local|tftp://hostIP/filename}`
Mode	Global Config

ip dhcp snooping database write-delay

Use this command to configure the interval in seconds at which the DHCP Snooping database will be persisted. The interval value ranges from 15 to 86400 seconds.

Default	300 seconds
Format	`ip dhcp snooping database write-delay <in seconds>`
Mode	Global Config

no ip dhcp snooping database write-delay

Use this command to set the write delay value to the default value.

Format	`no ip dhcp snooping database write-delay`
Mode	Global Config

ip dhcp snooping binding

Use this command to configure static DHCP Snooping binding.

Format	`ip dhcp snooping binding <mac-address> vlan <vlan id> <ip address> interface <interface id>`
Mode	Global Config

no ip dhcp snooping binding <mac-address>

Use this command to remove the DHCP static entry from the DHCP Snooping database.

Format	`no ip dhcp snooping binding <mac-address>`
Mode	Global Config

ip verify binding

Use this command to configure static IP source guard (IPSG) entries.

Format	`ip verify binding <`*`mac-address`*`> vlan <`*`vlan id`*`> <`*`ip address`*`> interface <`*`interface id`*`>`
Mode	Global Config

no ip verify binding

Use this command to remove the IPSG static entry from the IPSG database.

Format	`no ip verify binding <`*`mac-address`*`> vlan <`*`vlan id`*`> <`*`ip address`*`> interface <`*`interface id`*`>`
Mode	Global Config

ip dhcp snooping limit

Use this command to control the rate at which the DHCP Snooping messages come. The default rate is 15 pps with a range from 0 to 30 pps. The default burst level is 1 second with a range of 1 to 15 seconds.

Default	15 pps for rate limiting and 1 sec for burst interval
Format	`ip dhcp snooping limit {rate pps [burst interval seconds]}`
Mode	Interface Config

no ip dhcp snooping limit

Use this command to set the rate at which the DHCP Snooping messages come, and the burst level, to the defaults.

Format	`no ip dhcp snooping limit`
Mode	Interface Config

ip dhcp snooping log-invalid

Use this command to control the logging DHCP messages filtration by the DHCP Snooping application.

Default	disabled
Format	`ip dhcp snooping log-invalid`
Mode	Interface Config

no ip dhcp snooping log-invalid

Use this command to disable the logging DHCP messages filtration by the DHCP Snooping application.

Format	`no ip dhcp snooping log-invalid`
Mode	Interface Config

ip dhcp snooping trust

Use this command to configure the port as trusted.

Default	disabled
Format	`ip dhcp snooping trust`
Mode	Interface Config

no ip dhcp snooping trust

Use this command to configure the port as untrusted.

Format	`no ip dhcp snooping trust`
Mode	Interface Config

ip verify source

Use this command to configure the IPSG source ID attribute to filter the data traffic in the hardware. Source ID is the combination of IP address and MAC address. Normal command allows data traffic filtration based on the IP address. With the “port-security” option, the data traffic will be filtered based on the IP and MAC addresses.

Default	`the source ID is the IP address`
Format	`ip verify source {port-security}`
Mode	Interface Config

no ip verify source

Use this command to disable the IPSG configuration in the hardware. You cannot disable port-security alone if it is configured.

Format	`no ip verify source`
Mode	Interface Config

show ip dhcp snooping

Use this command to display the DHCP Snooping global configurations and per port configurations.

Format	`show ip dhcp snooping`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	The interface for which data is displayed.
Trusted	If it is enabled, DHCP snooping considers the port as trusted. The factory default is disabled.
Log Invalid Pkts	If it is enabled, DHCP snooping application logs invalid packets on the specified interface.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip dhcp snooping

DHCP snooping is Disabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
11 - 30, 40

Interface   Trusted    Log Invalid Pkts
---------   --------   ----------------
0/1          Yes             No
0/2          No             Yes
0/3          No             Yes
0/4          No              No
0/6          No              No
```

show ip dhcp snooping binding

Use this command to display the DHCP Snooping binding entries. To restrict the output, use the following options:

- Dynamic: Restrict the output based on DCHP snooping.
- Interface: Restrict the output based on a specific interface.
- Static: Restrict the output based on static entries.
- VLAN: Restrict the output based on VLAN.

Format	`show ip dhcp snooping binding [{static/dynamic}] [interface` *`unit/slot/port`*`] [`*`vlan id`*`]`
Mode	• Privileged EXEC • User EXEC

Term	Definition
MAC Address	Displays the MAC address for the binding that was added. The MAC address is the key to the binding database.
IP Address	Displays the valid IP address for the binding rule.
VLAN	The VLAN for the binding rule.
Interface	The interface to add a binding into the DHCP snooping interface.

Term	Definition
Type	Binding type; statically configured from the CLI or dynamically learned.
Lease (sec)	The remaining lease time for the entry.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip dhcp snooping binding

Total number of bindings: 2

MAC Address          IP Address    VLAN  Interface  Type  Lease (Secs)
------------------  ------------  ----  ---------  ---- -------------
00:02:B3:06:60:80   210.1.1.3      10   0/1              86400
00:0F:FE:00:13:04   210.1.1.4      10   0/1              86400
```

show ip dhcp snooping database

Use this command to display the DHCP Snooping configuration related to the database persistency.

Format	`show ip dhcp snooping database`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Agent URL	Bindings database agent URL.
Write Delay	The maximum write time to write the database into local or remote.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip dhcp snooping database

agent url:  /10.131.13.79:/sai1.txt

write-delay:  5000
```

show ip dhcp snooping statistics

Use this command to list statistics for DHCP Snooping security violations on untrusted ports.

Format	`show ip dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	The IP address of the interface in unit/slot/port format.
MAC Verify Failures	Represents the number of DHCP messages that were filtered on an untrusted interface because of source MAC address and client HW address mismatch.
Client Ifc Mismatch	Represents the number of DHCP release and Deny messages received on the different ports than learned previously.
DHCP Server Msgs Rec’d	Represents the number of DHCP server messages received on Untrusted ports.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip dhcp snooping statistics

 Interface    MAC Verify   Client Ifc   DHCP Server
               Failures     Mismatch    Msgs Rec'd
-----------   ----------   ----------   -----------
1/0/2                  0            0             0
1/0/3                  0            0             0
1/0/4                  0            0             0
1/0/5                  0            0             0
1/0/6                  0            0             0
1/0/7                  0            0             0
1/0/8                  0            0             0
1/0/9                  0            0             0
1/0/10                 0            0             0
1/0/11                 0            0             0
1/0/12                 0            0             0
1/0/13                 0            0             0
1/0/14                 0            0             0
1/0/15                 0            0             0
1/0/16                 0            0             0
1/0/17                 0            0             0
1/0/18                 0            0             0
1/0/19                 0            0             0
```

```
1/0/20                 0            0             0
```

clear ip dhcp snooping binding

Use this command to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format	`clear ip dhcp snooping binding [interface <`*`unit/slot/port`*`>]`
Mode	• Privileged EXEC • User EXEC

clear ip dhcp snooping statistics

Use this command to clear all DHCP Snooping statistics.

Format	`clear ip dhcp snooping statistics`
Mode	• Privileged EXEC • User EXEC

show ip verify source

Use this command to display the IPSG configurations on all ports.

Format	`show ip verify source`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Interface	Interface address in unit/slot/port format.
Filter Type	Is one of two values: • ip-mac: User has configured MAC address filtering on this interface. • ip: Only IP address filtering on this interface.
IP Address	IP address of the interface

Term	Definition
MAC Address	If MAC address filtering is not configured on the interface, the MAC Address field is empty. If port security is disabled on the interface, then the MAC Address field displays “permit-all.”
VLAN	The VLAN for the binding rule.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip verify source

Interface  Filter Type    IP Address       MAC Address      Vlan
---------  -----------  ---------------  -----------------  -----
    0/1     ip-mac       210.1.1.3       00:02:B3:06:60:80     10
    0/1     ip-mac       210.1.1.4       00:0F:FE:00:13:04     10
```

show ip source binding

Use this command to display the IPSG bindings.

Format	`show ip source binding [{static/dynamic}] [interface` *`unit/slot/port`*`]`
	`[`*`vlan id`*`]`

Mode	• Privileged EXEC • User EXEC

Term	Definition
MAC Address	The MAC address for the entry that is added.
IP Address	The IP address of the entry that is added.
Type	Entry type; statically configured from CLI or dynamically learned from DHCP Snooping.
VLAN	VLAN for the entry.
Interface	IP address of the interface in unit/slot/port format.

Example: The following shows example CLI display output for the command.

```
(switch) #show ip source binding

MAC Address       IP Address       Type         Vlan     Interface
-----------------  ---------------  -------------  -----  -------------
```

```
00:00:00:00:00:08         1.2.3.4  dhcp-snooping    2        1/0/1

00:00:00:00:00:09         1.2.3.4  dhcp-snooping    3        1/0/1

00:00:00:00:00:0A         1.2.3.4  dhcp-snooping    4        1/0/1
```

Dynamic ARP Inspection Commands

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

ip arp inspection vlan

Use this command to enable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Default	`disabled`
Format	`ip arp inspection vlan` *`vlan-list`*
Mode	Global Config

no ip arp inspection vlan

Use this command to disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection vlan` *`vlan-list`*
Mode	Global Config

ip arp inspection validate

Use this command to enable additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets. Each command overrides the configuration of the previous command. For example, if a command enables src-mac and dst-mac validations, and a second command enables IP validation only, the src-mac and dst-mac validations are disabled as a result of the second command.

Default	`disabled`
Format	`ip arp inspection validate {[src-mac] [dst-mac] [ip]}`
Mode	Global Config

no ip arp inspection validate

Use this command to disable the additional validation checks on the received ARP packets.

Format	`no ip arp inspection validate {[src-mac] [dst-mac] [ip]}`
Mode	Global Config

ip arp inspection vlan logging

Use this command to enable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Default	`enabled`
Format	`ip arp inspection vlan` *`vlan-list`* `logging`
Mode	Global Config

no ip arp inspection vlan logging

Use this command to disable logging of invalid ARP packets on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection vlan` *`vlan-list`* `logging`
Mode	Global Config

ip arp inspection trust

Use this command to configure an interface as trusted for Dynamic ARP Inspection.

Default	`enabled`
Format	`ip arp inspection trust`
Mode	Interface Config

no ip arp inspection trust

Use this command to configure an interface as untrusted for Dynamic ARP Inspection.

Format	`no ip arp inspection trust`
Mode	Interface Config

ip arp inspection limit

Use this command to configure the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections.

Note: The user interface will accept a rate limit for a trusted interface, but the limit will not be enforced unless the interface is configured to be untrusted.

Default	`15 pps for rate and 1 second for burst-interval`
Format	`ip arp inspection limit {rate` *`pps`* `[burst interval` *`seconds`*`]	none}`
Mode	Interface Config

no ip arp inspection limit

Use this command to set the rate limit and burst interval values for an interface to the default values of 15 pps and 1 second, respectively.

Format	`no ip arp inspection limit`
Mode	Interface Config

ip arp inspection filter

Use this command to configure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

Default	`No ARP ACL is configured on a VLAN`
Format	`ip arp inspection filter` *`acl-name`* `vlan` *`vlan-list`* `[static]`
Mode	Global Config

no ip arp inspection filter

Use this command to unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges.

Format	`no ip arp inspection filter` *`acl-name`* `vlan` *`vlan-list`* `[static]`
Mode	Global Config

arp access-list

Use this command to create an ARP ACL.

Format	`arp access-list` *`acl-name`*
Mode	Global Config

no arp access-list

Use this command to delete a configured ARP ACL.

Format	`no arp access-list` *`acl-name`*
Mode	Global Config

permit ip host mac host

Use this command to configure a rule for a valid IP address and MAC address combination used in ARP packet validation.

Format	`permit ip host` *`sender-ip`* `mac host` *`sender-mac`*
Mode	ARP Access-list Config

no permit ip host mac host

Use this command to delete a rule for a valid IP and MAC combination.

Format	`no permit ip host` *`sender-ip`* `mac host` *`sender-mac`*
Mode	ARP Access-list Config

show ip arp inspection

Use this command to display the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the *vlan-list* argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the **source mac validation**, **destination mac validation** and **invalid IP validation** information.

Format	`show ip arp inspection [vlan <`*`vlan-list`*`>]`
Mode	• Privileged EXEC • User EXEC

Term	Definition
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

Example: The following shows example CLI display output for the command.

```
(Switch) #show ip arp inspection vlan 10-12

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan          Configuration    Log Invalid   ACL Name   Static flag
 ----          -------------    -----------   ---------  ----------
   10                Enabled        Enabled   H2         Enabled
   11               Disabled        Enabled
   12               Enabled        Disabled
```

show ip arp inspection statistics

Use this command to display the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format	`show ip arp inspection statistics [vlan` *`vlan-list`*`]`
Mode	• Privileged EXEC • User EXEC

Term	Definition
VLAN	The VLAN ID for each displayed row.
Forwarded	The total number of valid ARP packets forwarded in this VLAN.
Dropped	The total number of not valid ARP packets dropped in this VLAN.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.
ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

Example: The following shows example CLI display output for the command **show ip arp inspection statistics** which lists the summary of forwarded and dropped ARP packets on all DAI-enabled VLANs.

```
VLAN  Forwarded  Dropped
----  ---------  -------
  10         90       14
  20         10        3
```

Example: The following shows example CLI display output for the command **show ip arp inspection statistics vlan <*vlan-list*>**.

```
VLAN    DHCP      ACL       DHCP       ACL       Bad Src   Bad Dest   Invalid
        Drops    Drops     Permits    Permits     MAC       MAC         IP
----- -------- --------- ----------- --------- ---------- ----------- ---------
10      11        1          65         25          1         1         0
20      1         0           8          2          0         1         1
```

clear ip arp inspection statistics

Use this command to reset the statistics for Dynamic ARP Inspection on all VLANs.

Default none

Format `clear ip arp inspection statistics`

Mode Privileged EXEC

show ip arp inspection interfaces

Use this command to display the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a unit/slot/port interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format `show ip arp inspection interfaces [unit/slot/port]`

Mode
- Privileged EXEC
- User EXEC

Term	Definition
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds.

Example: The following shows example CLI display output for the command.

```
(Switch) #show ip arp inspection interfaces

 Interface     Trust State  Rate Limit  Burst Interval
                                   (pps)        (seconds)
 ---------------  -----------   ----------  ---------------
 0/1                Untrusted           15                1
 0/2                Untrusted           10               10
```

show arp access-list

Use this command to display the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format	`show arp access-list [`*`acl-name`*`]`
Mode	• Privileged EXEC • User EXEC

Example: The following shows example CLI display output for the command.

```
(Switch) #show arp access-list

ARP access list H2
    permit ip host 1.1.1.1 mac host 00:01:02:03:04:05
    permit ip host 1.1.1.2 mac host 00:03:04:05:06:07
ARP access list H3
ARP access list H4
    permit ip host 2.1.1.2 mac host 00:03:04:05:06:08
```

IGMP Snooping Configuration Commands

This section describes the commands you use to configure IGMP snooping. The software supports IGMP Versions 1, 2, and 3. The IGMP snooping feature can help conserve bandwidth because it allows the switch to forward IP multicast traffic only to connected hosts that request multicast traffic. IGMPv3 adds source filtering capabilities to IGMP versions 1 and 2.

set igmp

This command enables IGMP Snooping on the system (Global Config Mode) or an interface (Interface Config Mode). This command also enables IGMP snooping on a particular VLAN (VLAN Config Mode) and can enable IGMP snooping on all interfaces participating in a VLAN.

If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

The IGMP application supports the following activities:

- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.

- Flooding of unregistered multicast data packets to all ports in the VLAN.

Default	disabled
Format	`set igmp`
Mode	• Global Config • Interface Config

Format	`set igmp <`*`vlanid`*`>`
Mode	VLAN Config

no set igmp

This command disables IGMP Snooping on the system, an interface or a VLAN.

Format	`no set igmp`
Mode	• Global Config • Interface Config

Format	`no set igmp <`*`vlanid`*`>`
Mode	VLAN Config

set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface has IGMP Snooping enabled and you enable this interface for routing or enlist it as a member of a port-channel (LAG), IGMP Snooping functionality is disabled on that interface. IGMP Snooping functionality is re-enabled if you disable routing or remove port-channel (LAG) membership from an interface that has IGMP Snooping enabled.

Default	disabled
Format	`set igmp interfacemode`
Mode	Global Config

no set igmp interfacemode

This command disables IGMP Snooping on all interfaces.

Format	`no set igmp interfacemode`
Mode	Global Config

set igmp fast-leave

This command enables or disables IGMP Snooping fast-leave admin mode on a selected interface or VLAN. Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.

Default	disabled
Format	`set igmp fast-leave`
Mode	Interface Config

Format	`set igmp fast-leave <`*`vlan_id`*`>`
Mode	VLAN Config

no set igmp fast-leave

This command disables IGMP Snooping fast-leave admin mode on a selected interface.

Format	`no set igmp fast-leave`
Mode	Interface Config

Format	`no set igmp fast-leave <`*`vlan_id`*`>`
Mode	VLAN Config

set igmp groupmembership-interval

This command sets the IGMP Group Membership Interval time on a VLAN, one interface or all interfaces. The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.

Default	260 seconds
Format	`set igmp groupmembership-interval <2-3600>`
Mode	• Interface Config • Global Config

Format	`set igmp groupmembership-interval <vlan_id> <2-3600>`
Mode	VLAN Config

no set igmp groupmembership-interval

This command sets the IGMPv3 Group Membership Interval time to the default value.

Format	`no set igmp groupmembership-interval`
Mode	• Interface Config • Global Config

Format	`no set igmp groupmembership-interval <vlan_id>`
Mode	VLAN Config

set igmp maxresponse

This command sets the IGMP Maximum Response time for the system, or on a particular interface or VLAN. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the IGMP Query Interval time value. The range is 1 to 25 seconds.

Default	10 seconds

Format	`set igmp maxresponse <1-25>`
Mode	• Global Config • Interface Config

Format	`set igmp maxresponse <vlan_id> <1-25>`
Mode	VLAN Config

no set igmp maxresponse

This command sets the max response time (on the interface or VLAN) to the default value.

Format	`no set igmp maxresponse`
Mode	• Global Config • Interface Config

Format	`no set igmp maxresponse <vlan_id>`
Mode	VLAN Config

set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time. The time is set for the system, on a particular interface or VLAN. This is the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out, i.e. no expiration.

Default	0
Format	`set igmp mcrtrexpiretime <0-3600>`
Mode	• Global Config • Interface Config

Format	`set igmp mcrtrexpiretime <vlan_id> <0-3600>`
Mode	VLAN Config

no set igmp mcrtrexpiretime

This command sets the Multicast Router Present Expiration time to 0. The time is set for the system, on a particular interface or a VLAN.

Format	`no set igmp mcrtrexpiretime`
Mode	• Global Config • Interface Config

Format	`no set igmp mcrtrexpiretime <vlan_id>`
Mode	VLAN Config

set igmp mrouter

This command configures the VLAN ID (`<vlanId>`) that has the multicast router mode enabled.

Format	`set igmp mrouter <vlan_id>`
Mode	Interface Config

no set igmp mrouter

This command disables multicast router mode for a particular VLAN ID (`<vlan_id>`).

Format	`no set igmp mrouter <vlan_id>`
Mode	Interface Config

set igmp mrouter interface

This command configures the interface as a multicast router interface. When configured as a multicast router interface, the interface is treated as a multicast router interface in all VLANs.

Default	disabled
Format	`set igmp mrouter interface`
Mode	Interface Config

no set igmp mrouter interface

This command disables the status of the interface as a statically configured multicast router interface.

Format	`no set igmp mrouter interface`
Mode	Interface Config

ip igmpsnooping unknown-multicast

This command enables the filtering of unknown multicast packets to the VLAN. Packets with an unknown multicast address in the destination field will be dropped. This command is mainly used when IGMP snooping is enabled, to prevent flooding of unwanted multicast packets to every port.

Format	`ip igmpsnooping unknown-multicast`
Mode	Global Config

no ip igmpsnooping unknown-multicast

This command disables the filtering of unknown multicast packets. Unknown multicast packets will be flooded to all ports in the same VLAN.

Format	`no ip igmpsnooping unknown-multicast`
Mode	Global Config

show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled.

Format	`show igmpsnooping` *`[<unit/slot/port>	<vlan_id>]`*
Mode	Privileged EXEC

When the optional arguments *<unit/slot/port>* or *<vlan_id>* are not used, the command displays the following information:

Term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interface Enabled for IGMP Snooping	The list of interfaces on which IGMP Snooping is enabled.
VLANS Enabled for IGMP Snooping	The list of VLANS on which IGMP Snooping is enabled.

When you specify the *<unit/slot/port>* values, the following information appears:

Term	Definition
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the interface.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the interface.
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

When you specify a value for *<vlan_id>*, the following information appears:

Term	Definition
VLAN ID	The VLAN ID.
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.

Term	Definition
Group Membership Interval	The amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.This value may be configured.
Maximum Response Time	The amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.
Multicast Router Expiry Time	The amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

show igmpsnooping mrouter interface

This command displays information about statically configured ports.

Format	`show igmpsnooping mrouter interface <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
Multicast Router Attached	Indicates whether multicast router is statically enabled on the interface.
VLAN ID	The list of VLANs of which the interface is a member.

show igmpsnooping mrouter vlan

This command displays information about statically configured ports.

Format	`show igmpsnooping mrouter vlan <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
Interface	The port on which multicast router information is being displayed.
VLAN ID	The list of VLANs of which the interface is a member.

show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the MFDB table.

Format	`show mac-address-table igmpsnooping`
Mode	Privileged EXEC

Term	Definition
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address is displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol).
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

IGMP Snooping Querier Commands

IGMP Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the “IGMP Querier”. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts to the port where the end device is located.

This section describes commands used to configure and display information on IGMP Snooping Queriers on the network and, separately, on VLANs.

set igmp querier

Use this command to enable IGMP Snooping Querier on the system, using Global Config mode, or on a VLAN. Using this command, you can specify the IP Address that the Snooping Querier switch should use as the source address while generating periodic queries.

If a VLAN has IGMP Snooping Querier enabled and IGMP Snooping is operationally disabled on it, IGMP Snooping Querier functionality is disabled on that VLAN. IGMP Snooping functionality is re-enabled if IGMP Snooping is operational on the VLAN.

Note: The Querier IP Address assigned for a VLAN takes preference over global configuration.

The IGMP Snooping Querier application supports sending periodic general queries on the VLAN to solicit membership reports.

Default	disabled
Format	`set igmp querier [<vlan-id>] [address ipv4_address]`
Mode	• Global Config • VLAN Mode

no set igmp querier

Use this command to disable IGMP Snooping Querier on the system. Use the optional `address` parameter to reset the querier address to 0.0.0.0.

Format	`no set igmp querier [<vlan-id>] [address]`
Mode	• Global Config • VLAN Mode

set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time. It is the amount of time in seconds that the switch waits before sending another general query.

Default	disabled
Format	`set igmp querier query-interval <1-18000>`
Mode	Global Config

no set igmp querier query-interval

Use this command to set the IGMP Querier Query Interval time to its default value.

Format	`no set igmp querier query-interval`
Mode	Global Config

set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period. It is the time period that the switch remains in Non-Querier mode once it has discovered that there is a Multicast Querier in the network.

Default	60 seconds
Format	`set igmp querier timer expiry <60-300>`
Mode	Global Config

no set igmp querier timer expiry

Use this command to set the IGMP Querier timer expiration period to its default value.

Format	`no set igmp querier timer expiry`
Mode	Global Config

set igmp querier version

Use this command to set the IGMP version of the query that the snooping switch is going to send periodically.

Default	1
Format	`set igmp querier version <1-2>`
Mode	Global Config

no set igmp querier version

Use this command to set the IGMP Querier version to its default value.

Format	`no set igmp querier version`
Mode	Global Config

set igmp querier election participate

Use this command to enable the Snooping Querier to participate in the Querier Election process when it discovers the presence of another Querier in the VLAN. When this mode is enabled, if the Snooping Querier finds that the other Querier's source address is better (less) than the Snooping Querier's address, it stops sending periodic queries. If the Snooping Querier wins the election, then it will continue sending periodic queries.

Default	disabled
Format	`set igmp querier election participate`
Mode	VLAN Config

no set igmp querier election participate

Use this command to set the Snooping Querier not to participate in querier election but go into non-querier mode as soon as it discovers the presence of another querier in the same VLAN.

Format	`no set igmp querier election participate`
Mode	VLAN Config

show igmpsnooping querier

Use this command to display IGMP Snooping Querier information. Configured information is displayed whether or not IGMP Snooping Querier is enabled.

Format	`show igmpsnooping querier [{detail	vlan <`*`vlanid`*`>}]`
Mode	Privileged EXEC

When the optional argument <*vlanid*> is not used, the command displays the following information.

Field	Description
Admin Mode	Indicates whether or not IGMP Snooping Querier is active on the switch.
Admin Version	The version of IGMP that will be used while sending out the queries.
Querier Address	The IP Address which will be used in the IPv4 header while sending out IGMP queries. It can be configured using the appropriate command.
Query Interval	The amount of time in seconds that a Snooping Querier waits before sending out the periodic general query.
Querier Timeout	The amount of time to wait in the Non-Querier operational state before moving to a Querier state.

When you specify a value for <*vlanid*>, the following additional information appears.

Field	Description
VLAN Admin Mode	Indicates whether iGMP Snooping Querier is active on the VLAN.
VLAN Operational State	Indicates whether IGMP Snooping Querier is in “Querier” or “Non-Querier” state. When the switch is in *Querier* state, it will send out periodic general queries. When in *Non-Querier* state, it will wait for moving to Querier state and does not send out any queries.
VLAN Operational Max Response Time	Indicates the time to wait before removing a Leave from a host upon receiving a Leave request. This value is calculated dynamically from the Queries received from the network. If the Snooping Switch is in Querier state, then it is equal to the configured value.
Querier Election Participation	Indicates whether the IGMP Snooping Querier participates in querier election if it discovers the presence of a querier in the VLAN.
Querier VLAN Address	The IP address will be used in the IPv4 header while sending out IGMP queries on this VLAN. It can be configured using the appropriate command.
Operational Version	The version of IPv4 will be used while sending out IGMP queries on this VLAN.
Last Querier Address	Indicates the IP address of the most recent Querier from which a Query was received.
Last Querier Version	Indicates the IGMP version of the most recent Querier from which a Query was received on this VLAN.

When the optional argument *detail* is used, the command shows the global information and the information for all Querier-enabled VLANs.

Default	disabled
Format	set mld
Mode	Global Config Interface Config

Format	no set mld <vlanid>
Mode	VLAN Mode

Default	disabled
Format	set mld fast-leave <*vlanid*>
Mode	• VLAN Mode

Format	no set mld fast-leave <*vlanid*>
Mode	• VLAN Mode

Default	260 seconds
Format	set mld groupmembership-interval <*2-3600*>
Mode	• Interface Config • Global Config

Format	no set mld groupmembership-interval <vlanid>
Mode	• VLAN Mode

Default	10 seconds
Format	set mld maxresponse <*1-65*>
Mode	• Global Config • Interface Config

Format	no set mld maxresponse
Mode	• Global Config • Interface Config

Default	0
Format	set mld mcrtexpiretime <*0-3600*>
Mode	• Global Config • Interface Config

Format	`no set mld mcrtexpiretime`
Mode	• Global Config • Interface Config

Default	disabled
Format	`set mld querier <address` *`ipv6_address`*`>`
Mode	• Global Config

Format	`no set mld querier address`
Mode	• Global Config

Port Security Commands

This section describes the command you use to configure Port Security on the switch. Port security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a port. Packets with a matching source MAC address are forwarded normally, and all other packets are discarded.

Note: To enable the SNMP trap specific to port security, see "snmp-server enable traps violation" on page 7-51.

port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config).

Default	disabled
Format	`port-security`
Mode	• Global Config • Interface Config

no port-security

This command disables port locking for one (Interface Config) or all (Global Config) ports.

Format	`no port-security`
Mode	• Global Config • Interface Config

port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Default	600
Format	`port-security max-dynamic <maxvalue>`
Mode	Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format	`no port-security max-dynamic`
Mode	Interface Config

port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a port.

Default	20
Format	`port-security max-static <maxvalue>`
Mode	Interface Config

no port-security max-static

This command sets maximum number of statically locked MAC addresses to the default value.

Format	`no port-security max-static`
Mode	Interface Config

port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses. The *<vid>* is the VLAN ID.

Format	`port-security mac-address <mac-address> <vid>`
Mode	Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format	`no port-security mac-address <mac-address> <vid>`
Mode	Interface Config

port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

Format	`port-security mac-address move`
Mode	Interface Config

show port-security

This command displays the port-security settings. If you do not use a parameter, the command displays the settings for the entire system. Use the optional parameters to display the settings on a specific interface or on all interfaces.

Format	`show port-security [{<unit/slot/port>	all}]`
Mode	Privileged EXEC

Term	Definition
Admin Mode	Port Locking mode for the entire system. This field displays if you do not supply any parameters.

For each interface, or for the interface you specify, the following information appears:

Term	Definition
Admin Mode	Port Locking mode for the Interface.
Dynamic Limit	Maximum dynamically allocated MAC Addresses.
Static Limit	Maximum statically allocated MAC Addresses.
Violation Trap Mode	Whether violation traps are enabled.

show port-security dynamic

This command displays the dynamically locked MAC addresses for the port.

Format	`show port-security dynamic <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of dynamically locked MAC.

show port-security static

This command displays the statically locked MAC addresses for port.

Format	`show port-security static <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of statically locked MAC.

show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format	`show port-security violation <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
MAC Address	MAC Address of discarded packet on locked port.

LLDP (802.1AB) Commands

This section describes the command you use to configure Link Layer Discovery Protocol (LLDP), which is defined in the IEEE 802.1AB specification. LLDP allows stations on an 802 LAN to advertise major capabilities and physical descriptions. The advertisements allow a network management system (NMS) to access and display this information.

lldp transmit

Use this command to enable the LLDP advertise capability.

Default	enabled
Format	`lldp transmit`
Mode	Interface Config

no lldp transmit

Use this command to return the local data transmission capability to the default.

Format	`no lldp transmit`
Mode	Interface Config

lldp receive

Use this command to enable the LLDP receive capability.

Default	enabled
Format	`lldp receive`
Mode	Interface Config

no lldp receive

Use this command to return the reception of LLDPDUs to the default value.

Format	`no lldp receive`
Mode	Interface Config

lldp timers

Use this command to set the timing parameters for local data transmission on ports enabled for LLDP. The *`<interval-seconds>`* determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 1-32768 seconds. The *`<hold-value>`* is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The *`<reinit-seconds>`* is the delay before re-initialization, and the range is 1-0 seconds.

Default	• interval—30 seconds • hold—4 • reinit—2 seconds

Format	`lldp timers` *`[interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>`*]
Mode	Global Config

no lldp timers

Use this command to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format	`no lldp timers` *`[interval] [hold] [reinit]`*
Mode	Global Config

lldp transmit-tlv

Use this command to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use *`sys-name`* to transmit the system name TLV. To configure the system name, see "snmp-server" on page 7-47. Use *`sys-desc`*to transmit the system description TLV. Use *`sys-cap`* to transmit the system capabilities TLV. Use *`port-desc`* to transmit the port description TLV. To configure the port description, see See "description" on page 3-5.

Default	all optional TLVs are included
Format	`lldp transmit-tlv` *`[sys-desc] [sys-name] [sys-cap] [port-desc]`*
Mode	Interface Config

no lldp transmit-tlv

Use this command to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format	`no lldp transmit-tlv` *`[sys-desc] [sys-name] [sys-cap] [port-desc]`*
Mode	Interface Config

lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs.

Default	enabled
Format	`lldp transmit-mgmt`
Mode	Interface Config

no lldp transmit-mgmt

Use this command to include transmission of the local system management address information in the LLDPDUs. Use this command to cancel inclusion of the management information in LLDPDUs.

Format	`no lldp transmit-mgmt`
Mode	Interface Config

lldp notification

Use this command to enable remote data change notifications.

Default	disabled
Format	`lldp notification`
Mode	Interface Config

no lldp notification

Use this command to disable notifications.

Default	disabled
Format	`no lldp notification`
Mode	Interface Config

lldp notification-interval

Use this command to configure how frequently the system sends remote data change notifications. The `<interval>` parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Default	5
Format	`lldp notification-interval <interval>`
Mode	Global Config

no lldp notification-interval

Use this command to return the notification interval to the default value.

Format	`no lldp notification-interval`
Mode	Global Config

clear lldp statistics

Use this command to reset all LLDP statistics, including MED-related information.

Format	`clear lldp statistics`
Mode	Privileged Exec

clear lldp remote-data

Use this command to delete all information from the LLDP remote data table, including MED-related information.

Format	`clear lldp remote-data`
Mode	Global Config

show lldp

Use this command to display a summary of the current LLDP configuration.

Format	`show lldp`
Mode	Privileged Exec

Term	Definition
Transmit Interval	How frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	The multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Re-initialization Delay	The delay before re-initialization, in seconds.
Notification Interval	How frequently the system sends remote data change notifications, in seconds.

show lldp interface

Use this command to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format	`show lldp interface {<unit/slot/port> | all}`
Mode	Privileged Exec

Term	Definition
Interface	The interface in a unit/slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

show lldp statistics

Use this command to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format	`show lldp statistics` *{<unit/slot/port> | all}*
Mode	Privileged Exec

Term	Definition
Last Update	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

The table contains the following column headings:

Term	Definition
Interface	The interface in unit/slot/port format.
Transmit Total	Total number of LLDP packets transmitted on the port.
Receive Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageouts	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TLV Discards	The number of TLVs discarded.
TLV Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV MED	Total number of LLDP MED TLVs received on the local ports.
TVL802.1	Total number of 802.1 LLDP TLVs received on the local ports.
TVL802.3	Total number of 802.3 LLDP TLVs received on the local ports.

show lldp remote-device

Use this command to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format	`show lldp remote-device {<unit/slot/port>	all}`
Mode	Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
RemID	An internal identifier to the switch to mark each remote device to the system.
Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.

Example: The following shows example CLI display output for the command.

```
(switch) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System Name
-------  -------   --------------------  ------------------  ------------------
0/1
0/2
0/3
0/4
0/5
0/6
0/7        2       00:FC:E3:90:01:0F     00:FC:E3:90:01:11
0/7        3       00:FC:E3:90:01:0F     00:FC:E3:90:01:12
0/7        4       00:FC:E3:90:01:0F     00:FC:E3:90:01:13
0/7        5       00:FC:E3:90:01:0F     00:FC:E3:90:01:14
0/7        1       00:FC:E3:90:01:0F     00:FC:E3:90:03:11
0/7        6       00:FC:E3:90:01:0F     00:FC:E3:90:04:11
0/8
0/9
0/10
0/11
0/12
--More-- or (q)uit
```

show lldp remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format	`show lldp remote-device detail <`*`unit/slot/port`*`>`
Mode	Privileged EXEC

Term	Definition
Local Interface	The interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the remote device.
Port ID Subtype	The type of port on the remote device.

Term	Definition
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	The amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.

Example: The following shows example CLI display output for the command.

```
(Switch) #show lldp remote-device detail 0/7

LLDP Remote Device Detail

Local Interface: 0/7


Remote Identifier: 2
Chassis ID Subtype: MAC Address
Chassis ID: 00:FC:E3:90:01:0F
Port ID Subtype: MAC Address
Port ID: 00:FC:E3:90:01:11
System Name:
System Description:
Port Description:
System Capabilities Supported:
System Capabilities Enabled:
Time to Live: 24 seconds
```

show lldp local-device

Use this command to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format	`show lldp local-device {<unit/slot/port> | all}`
Mode	Privileged EXEC

Term	Definition
Interface	The interface in a unit/slot/port format.
Port ID	The port ID associated with this interface.
Port Description	The port description associated with the interface.

show lldp local-device detail

Use this command to display detailed information about the LLDP data a specific interface transmits.

Format	`show lldp local-device detail <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
Interface	The interface that sends the LLDPDU.
Chassis ID Subtype	The type of identification used in the Chassis ID field.
Chassis ID	The chassis of the local device.
Port ID Subtype	The type of port on the local device.
Port ID	The port number that transmitted the LLDPDU.
System Name	The system name of the local device.
System Description	Describes the local system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format.
System Capabilities Supported	Indicates the primary function(s) of the device.

Term	Definition
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	The type of address and the specific address the local LLDP agent uses to send and receive information.

LLDP-MED Commands

Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) (ANSI-TIA-1057) provides an extension to the LLDP standard. Specifically, LLDP-MED provides extensions for network configuration and policy, device location, Power over Ethernet (PoE) management and inventory management.

lldp med

Use this command to enable MED. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default	enabled
Format	`lldp med`
Mode	Interface Config

no lldp med

Use this command to disable MED.

Format	`no lldp med`
Mode	Interface Config

lldp med confignotification

Use this command to configure all the ports to send the topology change notification.

Default	enabled
Format	`lldp med confignotification`
Mode	Interface Config

no ldp med confignotification

Use this command to disable notifications.

Format	`no lldp med confignotification`
Mode	Interface Config

lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Interface Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv` *`[capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`*
Mode	Interface Config

lldp med all

Use this command to configure LLDP-MED on all the ports

Format	`lldp med all`
Mode	Global Config

no lldp med all

Use this command to remove LLDP-MD on all ports.

Format	`no lldp med all`
Mode	Global Config

lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Format	`lldp med confignotification all`
Mode	Global Config

no lldp med confignotification all

Use this command to disable all the ports to send the topology change notification.

Format	`no lldp med confignotification all`
Mode	Global Config

lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count. `[count]` is the number of LLDP PDUs that will be transmitted when the product is enabled. The range is 1 to 10.

Default	3
Format	`lldp med faststartrepeatcount` *`[count]`*
Mode	Global Config

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format	`no lldp med faststartrepeatcount`
Mode	Global Config

lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default	By default, the capabilities and network policy TLVs are included.
Format	`lldp med transmit-tlv all [capabilities] [ex-pd] [ex-pse] [inventory] [location] [network-policy]`
Mode	Global Config

Term	Definition
capabilities	Transmit the LLDP capabilities TLV.
ex-pd	Transmit the LLDP extended PD TLV.
ex-pse	Transmit the LLDP extended PSE TLV.
inventory	Transmit the LLDP inventory TLV.
location	Transmit the LLDP location TLV.
network-policy	Transmit the LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format	`no lldp med transmit-tlv all [capabilities] [network-policy] [ex-pse] [ex-pd] [location] [inventory]`
Mode	Global Config

show lldp med

Use this command to display a summary of the current LLDP MED configuration.

Format	`show lldp med`
Mode	Privileged Exec

Term	**Definition**
Fast Start Repeat Count	The number of LLDP PDUs that will be transmitted when the protocol is enabled.
Device Class	The local device's MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic[IP Communication Controller etc.], Class II Media Conference Bridge etc.], Class III Communication [IP Telephone etc.]. Class IV Network Connectivity Device, which is typically a LAN Switch, Router, IEEE 802.11 Wireless Access Point, etc.

Example: The following shows example CLI display output for the command.

```
(switch) #show lldp med
LLDP MED Global Configuration

Fast Start Repeat Count:  3
Device Class:  Network Connectivity

(switch) #
```

show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface. *`<unit/slot/port>`* indicates a specific physical interface. *`all`* indicates all valid LLDP interfaces.

Format	`show lldp med interface {<unit/slot/port>	all}`
Mode	Privileged Exec

Term	Definition
Interface	The interface in a unit/slot/port format.
Link	Shows whether the link is up or down.
ConfigMED	Shows if the LLPD-MED mode is enabled or disabled on this interface
OperMED	Shows if the LLPD-MED TLVs are transmitted or not on this interface.
ConfigNotify	Shows if the LLPD-MED topology notification mode of this interface.
TLVsTx	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Capabilities), 1 (Network Policy), 2 (Location), 3 (Extended PSE), 4 (Extended Pd), or 5 (Inventory).

Example: The following shows example CLI display output for the command.

```
(Switch) #show lldp med interface all

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/1      Down    Disabled  Disabled  Disabled     0,1
1/0/2      Up      Disabled  Disabled  Disabled     0,1
1/0/3      Down    Disabled  Disabled  Disabled     0,1
1/0/4      Down    Disabled  Disabled  Disabled     0,1
1/0/5      Down    Disabled  Disabled  Disabled     0,1
1/0/6      Down    Disabled  Disabled  Disabled     0,1
1/0/7      Down    Disabled  Disabled  Disabled     0,1
1/0/8      Down    Disabled  Disabled  Disabled     0,1
1/0/9      Down    Disabled  Disabled  Disabled     0,1
1/0/10     Down    Disabled  Disabled  Disabled     0,1
1/0/11     Down    Disabled  Disabled  Disabled     0,1
1/0/12     Down    Disabled  Disabled  Disabled     0,1
1/0/13     Down    Disabled  Disabled  Disabled     0,1
1/0/14     Down    Disabled  Disabled  Disabled     0,1
```

```
TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory
--More-- or (q)uit
(Switch) #show lldp med interface 1/0/2

Interface  Link    configMED operMED   ConfigNotify TLVsTx
---------  ------  --------- --------  ------------ -----------
1/0/2      Up      Disabled  Disabled  Disabled     0,1

TLV Codes: 0- Capabilities,       1- Network Policy
           2- Location,           3- Extended PSE
           4- Extended Pd,        5- Inventory

(Routing) #
```

show lldp med local-device detail

This command displays detailed information about the LLDP data a specific interface transmits.

Format	`show lldp med local-device detail` *<unit/slot/port>*
Mode	Privileged EXEC

Term	Definition
Media Application Type	Shows the application type. Types are unknown, voice, voicesignaling, guestvoice, guestvoicesignaling, sfotphonevoice, videoconferencing, streamingvideo, videosignaling.
Vlan ID	Shows the VLAN id associated with a particular policy type
Priority	Shows the priority associated with a particular policy type.
DSCP	Shows the DSCP associated with a particular policy type.
Unknown	Indicates if the policy type is unknown. In this case, the VLAN ID, Priority and DSCP are ignored.
Tagged	Indicates if the policy type is using tagged or untagged VLAN.
Hardware Rev	Shows the local hardware version.
Firmware Rev	Shows the local firmware version.
Software Rev	Shows the local software version.
Serial Num	Shows the local serial number.
Mfg Name	Shows the manufacture name.
Model Name	Shows the model name.

Example: The following shows example CLI display output for the command.

```
(Switch) #show lldp med local-device detail 1/0/8

LLDP MED Local Device Detail

Interface: 1/0/8

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True


Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
```

```
Source: local
Priority: low
```

show lldp med remote-device

This command displays summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format `show lldp med remote-device {<unit/slot/port> | all}`

Mode Privileged EXEC

Term	Definition
Interface	The interface in a unit/slot/port format.
Device Class	The Remote device’s MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as Class I Generic [IP Communication Controller etc.], Class II Media [Conference Bridge etc.], Class III Communication [IP Telephone etc]). The fourth device is Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point etc.

Example: The following shows example CLI display output for the command.

```
(Switch) #show lldp med remote-device all

LLDP MED Remote Device Summary

Local
Interface  Remote ID  Device Class
---------  ---------  ------------
1/0/8        1         Class I
1/0/9        2         Not Defined
1/0/10       3         Class II
1/0/11       4         Class III
1/0/12       5         Network Con
```

show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format	`show lldp med remote-device detail <unit/slot/port>`
Mode	Privileged EXEC

Term	Definition
Supported Capabilities	Shows the suppoted capabilities that were received in MED TLV on this port.
Enabled capabilities	Shows the enabled capabilities that were enabled in MED TLV on this port.
Device Class	Shows the device class as advertized by the device remotely connected to the port.
Network Policy Information	Shows if network policy TLV is received in the LLDP frames on this port.
Media Application Type	Shows the application type. Types of applications are unknown, voice, voicesignaling, guestvoice, guestvoicesignaling, sfotphonevoice, videoconferencing, streamingvideo, videosignaling.
VLAN Id	Shows the VLAN id associated with a particular policy type.
Priority	Shows the priority associated with a particular policy type.
DSCP	Shows the DSCP associated with a particular policy type.
Unknown	Indicates if the policy type is unknown. In this case, the VLAN id, Priority and DSCP are ignored.
Tagged	Indicates if the policy type is using tagged or untagged VLAN.
Hardware Revision	Shows the hardware version of the remote device.
Firmware Revision	Shows the firmware version of the remote device.
Software Revision	Shows the software version of the remote device.
Serial Number	Shows the serial number of the remote device.
Manufacturer Name	Shows the manufacture name of the remote device.
Model Name	Shows the model name of the remote device.
Asset ID	Shows the asset id of the remote device.

Term	Definition
Sub Type	Shows the type of location information.
Location Information	Shows the location information as a string for a given type of location id
Device Type	Shows the remote device’s PoE device type connected to this port.
Available	Shows the remote port’s PSE power value in tenths of a watt.
Source	Shows the remote port’s PSE power source.
Priority	Shows the remote port’s PSE priority.
Required	Shows the remote port’s PD power requirement.
Source	Shows the remote port’s PD power source.
Priority	Shows the remote port’s PD power priority.

Example: The following shows example CLI display output for the command.

```
(Switch) #show lldp med remote-device detail 1/0/8

LLDP MED Remote Device Detail

Local Interface: 1/0/8
Remote Identifier: 18
Capabilities
MED Capabilities Supported: capabilities, networkpolicy, location, extendedpse
MED Capabilities Enabled: capabilities, networkpolicy
Device Class: Endpoint Class I

Network Policies
Media Policy Application Type : voice
Vlan ID: 10
Priority: 5
DSCP: 1
Unknown: False
Tagged: True

Media Policy Application Type : streamingvideo
Vlan ID: 20
Priority: 1
DSCP: 2
Unknown: False
Tagged: True

Inventory
Hardware Rev: xxx xxx xxx
Firmware Rev: xxx xxx xxx
```

```
Software Rev: xxx xxx xxx
Serial Num: xxx xxx xxx
Mfg Name: xxx xxx xxx
Model Name: xxx xxx xxx
Asset ID: xxx xxx xxx

Location
Subtype: elin
Info: xxx xxx xxx

Extended POE
Device Type: pseDevice

Extended POE PSE
Available: 0.3 Watts
Source: primary
Priority: critical

Extended POE PD

Required: 0.2 Watts
Source: local
Priority: low
```

Denial of Service Commands

This section describes the commands you use to configure Denial of Service (DoS) Control. The software provides support for classifying and blocking specific types of Denial of Service attacks. You can configure your system to monitor and block these types of attacks:

- **SIP=DIP:** Source IP address = Destination IP address.
- **First Fragment:**TCP Header size smaller then configured value.
- **TCP Fragment:** IP Fragment Offset = 1.
- **TCP Flag:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port:** Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP:** Limiting the size of ICMP Ping packets.

dos-control all

This command enables Denial of Service protection checks globally.

Default	disabled
Format	`dos-control all`
Mode	Global Config

no dos-control all

This command disables Denial of Service prevention checks globally.

Format	`no dos-control all`
Mode	Global Config

dos-control sipdip

This command enables Source IP address = Destination IP address (SIP=DIP) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SIP=DIP, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control sipdip`
Mode	Global Config

no dos-control sipdip

This command disables Source IP address = Destination IP address (SIP=DIP) Denial of Service prevention.

Format	`no dos-control sipdip`
Mode	Global Config

dos-control firstfrag

This command enables Minimum TCP Header Size Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having a TCP Header Size smaller then the configured value, the packets will be dropped if the mode is enabled.The default is *`disabled.`* If you enable dos-control firstfrag, but do not provide a Minimum TCP Header Size, the system sets that value to *`20`*.

Default	disabled <20>
Format	`dos-control firstfrag` [<0-255>]
Mode	Global Config

no dos-control firstfrag

This command sets Minimum TCP Header Size Denial of Service protection to the default value of *`disabled`*.

Format	`no dos-control firstfrag`
Mode	Global Config

dos-control tcpfrag

This command enables TCP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having IP Fragment Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfrag`
Mode	Global Config

no dos-control tcpfrag

This command disabled TCP Fragment Denial of Service protection.

Format	`no dos-control tcpfrag`
Mode	Global Config

dos-control tcpflag

This command enables TCP Flag Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attacks. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflag`
Mode	Global Config

no dos-control tcpflag

This command sets disables TCP Flag Denial of Service protections.

Format	`no dos-control tcpflag`
Mode	Global Config

dos-control l4port

This command enables L4 Port Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having Source TCP/UDP Port Number equal to Destination TCP/UDP Port Number, the packets will be dropped if the mode is enabled.

➡	**Note:** Some applications mirror source and destination L4 ports - RIP for example uses 520 for both. If you enable dos-control l4port, applications such as RIP may experience packet loss which would render the application inoperable.

Default	disabled
Format	`dos-control l4port`
Mode	Global Config

no dos-control l4port

This command disables L4 Port Denial of Service protections.

Format	`no dos-control l4port`
Mode	Global Config

dos-control icmp

This command enables Maximum ICMP Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMP Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	`dos-control icmp [<0-1023>]`
Mode	Global Config

no dos-control icmp

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmp`
Mode	Global Config

dos-control smacdmac

This command enables Source MAC address = Destination MAC address (SMAC=DMAC) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with SMAC=DMAC, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control smacdmac`
Mode	Global Config

no dos-control smacdmac

This command disables Source MAC address = Destination MAC address (SMAC=DMAC) Denial of Service protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control tcpport

This command enables TCP L4 source = destination port number (Source TCP Port =Destination TCP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source TCP Port =Destination TCP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpport`
Mode	Global Config

no dos-control tcpport

This command disables TCP L4 source = destination port number (Source TCP Port =Destination TCP Port) Denial of Service protection.

Format	`no dos-control smacdmac`
Mode	Global Config

dos-control udpport

This command enables UDP L4 source = destination port number (Source UDP Port =Destination UDP Port) Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress with Source UDP Port =Destination UDP Port, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control udppport`
Mode	Global Config

no dos-control udpport

This command disables UDP L4 source = destination port number (Source UDP Port =Destination UDP Port) Denial of Service protection.

Format	`no dos-control udppport`
Mode	Global Config

dos-control tcpflagseq

This command enables TCP Flag and Sequence Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Flag SYN set and a source port less than 1024 or having TCP Control Flags set to 0 and TCP Sequence Number set to 0 or having TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0 or having TCP Flags SYN and FIN both set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpflagseq`
Mode	Global Config

no dos-control tcpflagseq

This command sets disables TCP Flag and Sequence Denial of Service protection.

Format	`no dos-control tcpflagseq`
Mode	Global Config

dos-control tcpoffset

This command enables TCP Offset Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP Header Offset equal to one (1), the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpoffset`
Mode	Global Config

no dos-control tcpoffset

This command disabled TCP Offset Denial of Service protection.

Format	`no dos-control tcpoffset`
Mode	Global Config

dos-control tcpsyn

This command enables TCP SYN and L4 source = 0-1023 Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flag SYN set and an L4 source port from 0 to 1023, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsyn`
Mode	Global Config

no dos-control tcpsyn

This command sets disables TCP SYN and L4 source = 0-1023 Denial of Service protection.

Format	`no dos-control tcpsyn`
Mode	Global Config

dos-control tcpsynfin

This command enables TCP SYN and FIN Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP flags SYN and FIN set, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpsynfin`
Mode	Global Config

no dos-control tcpsynfin

This command sets disables TCP SYN & FIN Denial of Service protection.

Format	`no dos-control tcpsynfin`
Mode	Global Config

dos-control tcpfinurgpsh

This command enables TCP FIN and URG and PSH and SEQ=0 checking Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control tcpfinurgpsh`
Mode	Global Config

no dos-control tcpfinurgpsh

This command sets disables TCP FIN and URG and PSH and SEQ=0 checking Denial of Service protections.

dos-control icmpv4

Format	`no dos-control tcpfinurgpsh`
Mode	Global Config

dos-control icmpv4

This command enables Maximum ICMPv4 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv4 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	`dos-control icmpv4` *<0-16384>*
Mode	Global Config

no dos-control icmpv4

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv4`
Mode	Global Config

dos-control icmpv6

This command enables Maximum ICMPv6 Packet Size Denial of Service protections. If the mode is enabled, Denial of Service prevention is active for this type of attack. If ICMPv6 Echo Request (PING) packets ingress having a size greater than the configured value, the packets will be dropped if the mode is enabled.

Default	disabled <512>
Format	`dos-control icmpv6` *<0-16384>*
Mode	Global Config

no dos-control icmpv6

This command disables Maximum ICMP Packet Size Denial of Service protections.

Format	`no dos-control icmpv6`
Mode	Global Config

dos-control icmpfrag

This command enables ICMP Fragment Denial of Service protection. If the mode is enabled, Denial of Service prevention is active for this type of attack. If packets ingress having fragmented ICMP packets, the packets will be dropped if the mode is enabled.

Default	disabled
Format	`dos-control icmpfrag`
Mode	Global Config

no dos-control icmpfrag

This command disabled ICMP Fragment Denial of Service protection.

Format	`no dos-control icmpfrag`
Mode	Global Config

show dos-control

This command displays Denial of Service configuration information.

Format	`show dos-control`
Mode	Privileged EXEC

➡	**Note:** Not all messages below are available in all 7000series managed switches.

Term	Definition
First Fragment Mode	May be enabled or disabled. The factory default is disabled.
Min TCP Hdr Size <0-255>	The factory default is 20.
ICMP Mode	May be enabled or disabled. The factory default is disabled.
Max ICMPv4 Pkt Size	The range is 0-1023. The factory default is 512.
Max ICMPv6 Pkt Size	The range is 0-16384. The factory default is 512.
ICMP Fragment Mode	May be enabled or disabled. The factory default is disabled.
L4 Port Mode	May be enabled or disabled. The factory default is disabled.
TCP Port Mode	May be enabled or disabled. The factory default is disabled.
UDP Port Mode	May be enabled or disabled. The factory default is disabled.
SIPDIP Mode	May be enabled or disabled. The factory default is disabled.
SMACDMAC Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag Mode	May be enabled or disabled. The factory default is disabled.
TCP FIN&URG& PSH Mode	May be enabled or disabled. The factory default is disabled.
TCP Flag & Sequence Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN Mode	May be enabled or disabled. The factory default is disabled.
TCP SYN & FIN Mode	May be enabled or disabled. The factory default is disabled.
TCP Fragment Mode	May be enabled or disabled. The factory default is disabled.
TCP Offset Mode	May be enabled or disabled. The factory default is disabled.

MAC Database Commands

This section describes the commands you use to configure and view information about the MAC databases.

bridge aging-time

This command configures the forwarding database address aging timeout in seconds. The `<seconds>` parameter must be within the range of 10 to 1,000,000 seconds.

Default	300
Format	`bridge aging-time <10-1,000,000>`
Mode	Global Config

no bridge aging-time

This command sets the forwarding database address aging timeout to the default value.

Format	`no bridge aging-time`
Mode	Global Config

show forwardingdb agetime

This command displays the timeout for address aging.

Default	all
Format	`show forwardingdb agetime`
Mode	Privileged EXEC

Term	Definition
Address Aging Timeout	• This parameter displays the address aging timeout for the associated forwarding database.

show mac-address-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If you enter the command with no parameter, the entire table is displayed. You can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format	`show mac-address-table multicast <macaddr>`
Mode	Privileged EXEC

Term	Definition
MAC Address	A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as a MAC address and VLAN ID combination of 8 bytes.
Type	The type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, GMRP, and Static Filtering.
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
Forwarding Interfaces	The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

show mac-address-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format	`show mac-address-table stats`
Mode	Privileged EXEC

Term	Definition
Max MFDB Table Entries	The total number of entries that can possibly be in the Multicast Forwarding Database table.
Most MFDB Entries Since Last Reset	The largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the MFDB.

ISDP Commands

This section describes the commands you use to configure the industry standard Discovery Protocol (ISDP).

isdp run

This command enables ISDP on the switch.

Default	Enabled
Format	`isdp run`
Mode	Global Config

no isdp run

This command disables ISDP on the switch.

Format	`no isdp run`
Mode	Global Config

isdp holdtime

This command configures the hold time for ISDP packets that the switch transmits. The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range is given in seconds.

Default	180 seconds
Format	`isdp holdtime <10-255>`
Mode	Global Config

isdp timer

This command sets the period of time between sending new ISDP packets. The range is given in seconds.

Default	30 seconds
Format	`isdp timer <5-254>`
Mode	Global Config

isdp advertise-v2

This command enables the sending of ISDP version 2 packets from the device.

Default	Enabled
Format	`isdp advertise-v2`
Mode	Global Config

no isdp advertise-v2

This command disables the sending of ISDP version 2 packets from the device.

Format	`no isdp advertise-v2`
Mode	Global Config

isdp enable

This command enables ISDP on the interface.

Default	Enabled
Format	`isdp enable`
Mode	Interface Config

no isdp enable

This command disables ISDP on the interface.

Format	`no isdp enable`
Mode	Interface Config

clear isdp counters

This command clears ISDP counters.

Format	`clear isdp counters`
Mode	Privileged EXEC

clear isdp table

This command clears entries in the ISDP table.

Format	`clear isdp table`
Mode	Privileged EXEC

show isdp

This command displays global ISDP settings.

Format	`show isdp`
Mode	Privileged EXEC

Term	Definition
Timer	The frequency with which this device sends ISDP packets. This value is given in seconds.
Hold Time	The length of time the receiving device should save information sent by this device. This value is given in seconds.
Version 2 Advertisements	The setting for sending ISDPv2 packets. If disabled, version 1 packets are transmitted.

Term	Definition
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of the Device ID Format object.
Device ID Format Capability	Indicates the Device ID format capability of the device. • `serialNumber` indicates that the device uses a serial number as the format for its Device ID. • `macAddress` indicates that the device uses a Layer 2 MAC address as the format for its Device ID. • `other` indicates that the device uses its platform-specific format as the format for its Device ID.
Device ID Format	Indicates the Device ID format of the device. • `serialNumber` indicates that the value is in the form of an ASCII string containing the device serial number. • `macAddress` indicates that the value is in the form of a Layer 2 MAC address. • `other` indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example, ASCII string contains serialNumber appended/prepended with system name.

show isdp interface

This command displays ISDP settings for the specified interface.

Format	`show isdp interface {all | <unit/slot/port>}`
Mode	Privileged EXEC

Term	Definition
Mode	ISDP mode enabled/disabled status for the interface(s).

show isdp entry

This command displays ISDP entries. If the device id is specified, then only entries for that device are shown.

Format	`show isdp entry  {all | deviceid}`
Mode	Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP address(es) associated with the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Version	The software version that the neighbor is running.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Capability	ISDP Functional Capabilities advertised by the neighbor.

show isdp neighbors

This command displays the list of neighboring devices.

Format	`show isdp neighbors [ {<unit/slot/port> |  detail} ]`
Mode	Privileged EXEC

Term	Definition
Device ID	The device ID associated with the neighbor which advertised the information.
IP Addresses	The IP addresses associated with the neighbor.
Capability	ISDP functional capabilities advertised by the neighbor.
Platform	The hardware platform advertised by the neighbor.
Interface	The interface (unit/slot/port) on which the neighbor's advertisement was received.
Port ID	The port ID of the interface from which the neighbor sent the advertisement.
Hold Time	The hold time advertised by the neighbor.
Advertisement Version	The version of the advertisement packet received from the neighbor.
Entry Last Changed Time	Displays when the entry was last modified.
Version	The software version that the neighbor is running.

Example: The following shows example CLI display output for the command.

```
(Switch) #show isdp neighbors detail

Device ID                     0001f45f1bc0
Address(es):
    IP Address:               10.27.7.57
Capability                    Router Trans Bridge Switch IGMP
Platform                      SecureStack C2
Interface                     0/48
Port ID                       ge.3.14
Holdtime                      131
Advertisement Version         2
Entry last changed time       0 days 00:01:59
Version :                     05.00.56
```

show isdp traffic

This command displays ISDP statistics.

Format	show isdp traffic
Mode	Privileged EXEC

Term	Definition
ISDP Packets Received	Total number of ISDP packets received
ISDP Packets Transmitted	Total number of ISDP packets transmitted
ISDPv1 Packets Received	Total number of ISDPv1 packets received
ISDPv1 Packets Transmitted	Total number of ISDPv1 packets transmitted
ISDPv2 Packets Received	Total number of ISDPv2 packets received
ISDPv2 Packets Transmitted	Total number of ISDPv2 packets transmitted
ISDP Bad Header	Number of packets received with a bad header
ISDP Checksum Error	Number of packets received with a checksum error
ISDP Transmission Failure	Number of packets which failed to transmit
ISDP Invalid Format	Number of invalid packets received
ISDP Table Full	Number of times a neighbor entry was not added to the table due to a full database

Term	Definition
ISDP IP Address Table Full	Displays the number of times a neighbor entry was added to the table without an IP address.

debug isdp packet

This command enables tracing of ISDP packets processed by the switch. ISDP must be enabled on both the device and the interface in order to monitor packets for a particular interface.

Format	`debug isdp packet [{receive	transmit}]`
Mode	Privileged EXEC

no debug isdp packet

This command disables tracing of ISDP packets on the receive or the transmit sides or on both sides.

Format	`no debug isdp packet [{receive	transmit}]`
Mode	Privileged EXEC

Priority-Based Flow control commands

Ordinarily, when flow control is enabled on a physical link, it applies to all traffic on the link. When congestion occurs, the hardware sends pause frames that temporarily suspend traffic flow. Pausing traffic helps prevent buffer overflow and dropped frames.

Priority-based flow control provides a way to distinguish which traffic on physical link is paused when congestion occurs, based on the priority of the traffic. An interface can be configured to pause only high priority (i.e., loss-sensitive) traffic when necessary to prevent dropped frames, while allowing traffic that has greater loss tolerance to continue to flow on the interface.

Priorities are differentiated by the priority field of the IEEE 802.1Q VLAN header, which identifies an IEEE 802.1p priority value. In FASTPATH, these priority values must be mapped to internal class-of-service (CoS) values.

To enable priority-based flow control for a particular CoS value on an interface:

- Ensure that VLAN tagging is enabled on the interface so that the 802.1p priority values are carried through the network.
- Ensure that 802.1p priority values are mapped to FASTPATH CoS values.
- Use the datacenter-bridging priority-flow-control mode on command to enable priority-based flow control on the the interface.
- Use the datacenter-bridging priority-flow-control priority command to specify the CoS values that should be paused ("no-drop") due to greater loss sensitivity. Unless configured as "no-drop", all CoS priorities are considered nonpausable ("drop") when priority-based flow control is enabled.

When priority-flow-control is disabled, the interface defaults to the IEEE 802.3x flow control setting for the interface. When priority-based flow control is enabled, the interface will not pause any CoS unless there is at least one no-drop priority.

datacenter-bridging priority-flow-control mode on

Use this command to enable priority-based flow control on an interface.

Format	`datacenter-bridging priority-flow-control mode on`
Mode	Interface Config
Default	Disabled

no datacenter-bridging priority-flow-control mode

Use this command to disable priority flow control on an interface.

Format	`no datacenter-bridging priority-flow-control`
Mode	Interface Config

datacenter-bridging priority-flow-control priority

Use this command to specify the priority group(s) that should be paused when necessary to prevent dropped frames; i.e., the group to receive priority flow control. This configuration has no effect on interfaces not enabled for priority flow control.

VLAN tagging must be enabled to carry the 802.1p value through the network. The number of lossless priorities supported on XSM7224S is 2.

Additionally, the mapping of class-of-service levels to 802.1p priority values to must be set to one-to-one.

Format	`datacenter-bridging priority-flow-control priority priority-list {drop | no-drop}`
Mode	Interface Config
Default	drop

show datacenter-bridging priority-flow-control

This command displays a summary of the priority flow control configuration for a specified interface or all interfaces.

Format	`show datacenter-bridging priority-flow-control [interface <unit/slot/port>]`
Mode	Privileged EXEC

```
(Switch) #show datacenter-bridging priority-flow-control

Port Drop No-Drop State Priorities Priorities
---- ---- ------ -------- -------
1/0/1 1-4,7 5,6 Enabled
1/0/2 1-4,6-7 5 Enabled
….
1/0/48 1-4,7 5,6 Enabled
```

Chapter 4
Routing Commands

This chapter describes the routing commands available in the 7000 series CLI.

The Routing Commands chapter contains the following sections:

Warning: The commands in this chapter are in one of three functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Clear commands clear some or all of the settings to factory defaults.

Address Resolution Protocol (ARP) Commands

This section describes the commands you use to configure ARP and to view ARP information on the switch. ARP associates IP addresses with MAC addresses and stores the information as ARP entries in the ARP cache.

arp

This command creates an ARP entry. The value for `<ipaddress>` is the IP address of a device on a subnet attached to an existing routing interface. `<macaddr>` is a unicast MAC address for that device.

The format of the MAC address is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format	**`arp`** `<ipaddress> <macaddr>`
Mode	Global Config

no arp

This command deletes an ARP entry. The value for `<arpentry>` is the IP address of the interface. The value for `<ipaddress>` is the IP address of a device on a subnet attached to an existing routing interface. `<macaddr>` is a unicast MAC address for that device.

Format	**`no arp`** `<ipaddress> <macaddr>`
Mode	Global Config

ip proxy-arp

This command enables proxy ARP on a router interface. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default	enabled
Format	`ip proxy-arp`
Mode	Interface Config

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format	`no ip proxy-arp`
Mode	Interface Config

arp cachesize

This command configures the ARP cache size. The ARP cache size value is a platform specific integer value. The default size also varies depending on the platform.

Format	**`arp cachesize`** *`<platform specific integer value>`*
Mode	Global Config

no arp cachesize

This command configures the default ARP cache size.

Format	`no arp cachesize`
Mode	Global Config

arp dynamicrenew

This command enables the ARP component to automatically renew dynamic ARP entries when they age out.

Default	enabled
Format	`arp dynamicrenew`
Mode	Privileged EXEC

no arp dynamicrenew

This command prevents dynamic ARP entries from renewing when they age out.

Format	`no arp dynamicrenew`
Mode	Privileged EXEC

arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format	**`arp purge`** *`<ipaddr>`*
Mode	Privileged EXEC

arp resptime

This command configures the ARP request response timeout.

The value for *`<seconds>`* is a valid positive integer, which represents the IP ARP entry response timeout time in seconds. The range for *`<seconds>`* is between 1-10 seconds.

Default	1
Format	**`arp resptime`** *`<1-10>`*
Mode	Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format	`no arp resptime`
Mode	Global Config

arp retries

This command configures the ARP count of maximum request for retries.

The value for *`<retries>`* is an integer, which represents the maximum number of request for retries. The range for *`<retries>`* is an integer between 0-10 retries.

Default	4
Format	**`arp retries`** *`<0-10>`*
Mode	Global Config

no arp retries

This command configures the default ARP count of maximum request for retries.

Format	`no arp retries`
Mode	Global Config

arp timeout

This command configures the ARP entry ageout time.

The value for `<seconds>` is a valid positive integer, which represents the IP ARP entry ageout time in seconds. The range for `<seconds>` is between 15-21600 seconds.

Default	1200
Format	**`arp timeout`** *`<15-21600>`*
Mode	Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format	`no arp timeout`
Mode	Global Config

clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* keyword is specified, the dynamic entries of type gateway are purged as well.

Format	**`clear arp-cache`** *`[gateway]`*
Mode	Privileged EXEC

clear arp-switch

Use this command to clear the contents of the switch's Address Resolution Protocol (ARP) table that contains entries learned through the Management port. To observe whether this command is successful, **`ping`** from the remote system to the DUT. Issue the **`show arp switch`** command to see the ARP entries. Then issue the **`clear arp-switch`** command and check the **`show arp switch`** entries. There will be no more arp entries.

Format	`clear arp-switch`
Mode	Privileged EXEC

show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the **`show arp`** results in conjunction with the **`show arp switch`** results.

Format	`show arp`
Mode	Privileged EXEC

Term	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Configured/Active / Max	The static entry count in the ARP table, the active entry count in the ARP table, the active entry count in the ARP table, and maximum static entry count in the ARP table.

The following are displayed for each ARP entry:

Term	Definition
IP Address	The IP address of a device on a subnet attached to an existing routing interface.

Term	Definition
MAC Address	The hardware MAC address of that device.
Interface	The routing unit/slot/port associated with the device ARP entry.
Type	The type that is configurable. The possible values are Local, Gateway, Dynamic and Static.
Age	The current age of the ARP entry since last refresh (in hh:mm:ss format)

show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format	`show arp brief`
Mode	Privileged EXEC

Term	Definition
Age Time (seconds)	The time it takes for an ARP entry to age out. This value is configurable. Age time is measured in seconds.
Response Time (seconds)	The time it takes for an ARP request timeout. This value is configurable. Response time is measured in seconds.
Retries	The maximum number of times an ARP request is retried. This value is configurable.
Cache Size	The maximum number of entries in the ARP table. This value is configurable.
Dynamic Renew Mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.
Total Entry Count Current / Peak	The total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Current / Max	The static entry count in the ARP table and maximum static entry count in the ARP table.

show arp switch

This command displays the contents of the switch’s Address Resolution Protocol (ARP) table.

Format	`show arp switch`
Mode	Privileged EXEC

Term	Definition
IP Address	The IP address of a device on a subnet attached to the switch.
MAC Address	The hardware MAC address of that device.
Interface	The routing unit/slot/port associated with the device's ARP entry.

IP Routing Commands

This section describes the commands you use to enable and configure IP routing on the switch.

routing

This command enables IPv4 and IPv6 routing for an interface. You can view the current value for this function with the **`show ip brief`** command. The value is labeled as "Routing Mode."

Default	disabled
Format	`routing`
Mode	Interface Config

no routing

This command disables routing for an interface.

You can view the current value for this function with the **`show ip brief`** command. The value is labeled as "Routing Mode."

Format	`no routing`
Mode	Interface Config

ip routing

This command enables the IP Router Admin Mode for the master switch.

Format	`ip routing`
Mode	Global Config

no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format	`no ip routing`
Mode	Global Config

ip address

This command configures an IP address on an interface. You can also use this command to configure one or more secondary IP addresses on the interface.The value for *`<ipaddr>`* is the IP address of the interface. The value for *`<subnetmask>`* is a 4-digit dotted-decimal number which represents the subnet mask of the interface. The subnet mask must have contiguous ones and be no longer than 30 bits, for example 255.255.255.0. This command adds the label IP address in **`show ip interface`**.

Format	**`ip address`** *`<ipaddr> <subnetmask> [secondary]`*
Mode	Interface Config

no ip address

This command deletes an IP address from an interface. The value for *`<ipaddr>`* is the IP address of the interface in a.b.c.d format where the range for a, b, c, and d is 1-255. The value for *`<subnetmask>`* is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses (primary and secondary) configured on the interface, enter the command **`no ip address`**.

Format	**`no ip address`** *`[{<ipaddr> <subnetmask> [secondary]}]`*
Mode	Interface Config

ip route

This command configures a static route. The *`<ipaddr>`* parameter is a valid IP address, and *`<subnetmask>`* is a valid subnet mask. The *`<nexthopip>`* parameter is a valid IP address of the next hop router. Specifying `Null0` as nexthop parameter adds a static reject route. The optional *`<preference>`* parameter is an integer (value from 1 to 255) that allows you to specify the preference value (sometimes called “administrative distance”) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, you control whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination. A route with a preference of 255 cannot be used to forward traffic.

For the static routes to be visible, you must perform the following steps:

- Enable ip routing globally.
- Enable ip routing for the interface.
- Confirm that the associated link is also up.

Default	preference—1
Format	`ip route` *`<ipaddr> <subnetmask> [<nexthopip>`* `| Null0`*`] [<preference>]`*
Mode	Global Config

no ip route

This command deletes a single next hop to a destination static route. If you use the *`<nexthopip>`* parameter, the next hop is deleted. If you use the *`<preference>`* value, the preference value of the static route is reset to its default.

Format	`no ip route` *`<ipaddr> <subnetmask> [{<nexthopip> [<preference>]`* `|`
	`Null0`*`}]`*

Mode	Global Config

ip route default

This command configures the default route. The value for *`<nexthopip>`* is a valid IP address of the next hop router. The *`<preference>`* is an integer value from 1 to 255. A route with a preference of 255 cannot be used to forward traffic.

Default	preference—1
Format	`ip route default` *`<nexthopip> [<preference>]`*
Mode	Global Config

no ip route default

This command deletes all configured default routes. If the optional *<nexthopip>* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

Format	**`no ip route default`** *`[{<nexthopip>	<preference>}]`*
Mode	Global Config

ip route distance

This command sets the default distance (preference) for static routes. Lower route distance values are preferred when determining the best route. The **`ip route`** and **`ip route default`** commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the **`ip route distance`** command.

Default	1
Format	**`ip route distance`** *`<1-255>`*
Mode	Global Config

no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format	`no ip route distance`
Mode	Global Config

ip netdirbcast

This command enables the forwarding of network-directed broadcasts. When enabled, network directed broadcasts are forwarded. When disabled they are dropped.

Default	disabled

Format	`ip netdirbcast`
Mode	Interface Config

no ip netdirbcast

This command disables the forwarding of network-directed broadcasts. When disabled, network directed broadcasts are dropped.

Format	`no ip netdirbcast`
Mode	Interface Config

ip mtu

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. The software currently does not fragment IP packets.

- Packets forwarded in hardware ignore the IP MTU.
- Packets forwarded in software are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack. The IP stack uses its default IP MTU and ignores the value set using the ip mtu command.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the **`ip ospf mtu-ignore`** command.)

Note: The IP MTU size refers to the maximum size of the IP packet (IP Header + IP payload). It does not include any extra bytes that may be required for Layer-2 headers. To receive and process packets, the Ethernet MTU (see "mtu" on page 3-5) must take into account the size of the Ethernet header.

Default	1500 bytes
Format	**`ip mtu`** *`<68-1500>`*
Mode	Interface Config

no ip mtu

This command resets the ip mtu to the default value.

Format	**`no ip mtu`** *`<mtu>`*
Mode	Interface Config

encapsulation

This command configures the link layer encapsulation type for the packet. The encapsulation type can be *`ethernet`* or *`snap`*.

Default	ethernet
Format	**`encapsulation`** *`{ethernet	snap}`*
Mode	Interface Config

➡ **Note:** Routed frames are always ethernet encapsulated when a frame is routed to a VLAN.

clear ip route all

This command removes all the route entries learned over the network.

Format	`clear ip route all`
Mode	Privileged EXEC
Protocol	Tells which protocol added the specified route. The possibilities are: local, static, OSPF, or RIP.
Total Number of Routes	The total number of routes.

show ip brief

This command displays all the summary information of the IP, including the ICMP rate limit configuration and the global ICMP Redirect configuration.

Format	`show ip brief`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Routing Mode	Shows whether the routing mode is enabled or disabled.
Maximum Next Hops	The maximum number of next hops the packet can travel.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. *Burst-interval* is from 0 to 2147483647 milliseconds. The default *burst-interval* is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.

The following shows example CLI display output for the command.

```
(Switch) #show ip brief

Default Time to Live........................... 64
Routing Mode................................... Disabled
Maximum Next Hops.............................. 4
Maximum Routes................................. 6000
ICMP Rate Limit Interval....................... 1000 msec
ICMP Rate Limit Burst Size..................... 100 messages
ICMP Echo Replies.............................. Enabled
ICMP Redirects................................. Enabled
```

show ip interface

This command displays all pertinent information about the IP interface.

Format	**`show ip interface {`***`<unit/slot/port>	vlan <1-4093>	loopback <0-7>}`*
Modes	• Privileged EXEC • User EXEC

Term	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the "ip helper-address (Global Config)command.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface.
Active State	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

The following shows example CLI display output for the command.

```
(switch)#show ip interface 1/0/2

Routing Interface Status....................... Down
Primary IP Address............................. 1.2.3.4/255.255.255.0
Secondary IP Address(es)....................... 21.2.3.4/255.255.255.0
............................................... 22.2.3.4/255.255.255.0
Helper IP Address.............................. 1.2.3.4
............................................... 1.2.3.5
```

```
Routing Mode................................... Disable
Administrative Mode............................ Enable
Forward Net Directed Broadcasts................ Disable
Proxy ARP...................................... Enable
Local Proxy ARP................................ Disable
Active State................................... Inactive
Link Speed Data Rate........................... Inactive
MAC Address.................................... 00:10:18:82:0C:68
Encapsulation Type............................. Ethernet
IP MTU......................................... 1500
Bandwidth...................................... 100000 kbps
Destination Unreachables....................... Enabled
ICMP Redirects................................. Enabled
```

show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router.

Format	`show ip interface brief`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
State	Routing operational state of the interface.
IP Address	The IP address of the routing interface in 32-bit dotted decimal format.
IP Mask	The IP mask of the routing interface in 32-bit dotted decimal format.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	The multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

show ip route

This command displays the routing table. The `<ip-address>` specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The `<mask>` specifies the subnet mask for the given `<ip-address>`. When you use the `longer-`

prefixes keyword, the *<ip-address>* and *<mask>* pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the *<protocol>* parameter to specify the protocol that installed the routes. The value for *<protocol>* can be *connected*, *ospf*, *rip*, or *static*. Use the *all* parameter to display all routes including best and non-best routes. If you do not use the *all* parameter, the command only displays the best route.

Note: If you use the *connected* keyword for *<protocol>*, the *all* option is not available because there are no best or non-best connected routes.

Format **show ip route** *[{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]*

Modes
- Privileged EXEC
- User EXEC

Term	Definition
Route Codes	The key for the routing protocol codes that might appear in the routing table output.

The **show ip route** command displays the routing tables in the following format:

```
Code   IP-Address/Mask [Preference/Metric] via Next-Hop, Route-Timestamp,
Interface
```

The columns for the routing table display the following information:

Term	Definition
Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Route-Timestamp	The last updated time for dynamic routes. The format of Route-Timestamp will be • Days:Hours:Minutes if days > = 1 • Hours:Minutes:Seconds if days < 1
Interface	The outgoing router interface to use when forwarding traffic to the next destination. For reject routes, the next hop interface would be Null0 interface.

To administratively control the traffic destined to a particular network and prevent it from being forwarded through the router, you can configure a static reject route on the router. Such traffic would be discarded and the ICMP destination unreachable message is sent back to the source. This is typically used for preventing routing loops. The reject route added in the RTO is of the type **OSPF Inter-Area**. Reject routes (routes of REJECT type installed by any protocol) are not redistributed by OSPF/RIP. Reject routes are supported in both OSPFv2 and OSPFv3.

The following shows example CLI display output for the command.

```
(Switch) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2

C 1.1.1.0/24 [0/1] directly connected, 0/11
C 2.2.2.0/24 [0/1] directly connected, 0/1
C 5.5.5.0/24 [0/1] directly connected, 0/5
S 7.0.0.0/8 [1/0] directly connected, Null0
OIA 10.10.10.0/24 [110/6] via 5.5.5.2,   00h:00m:01s,  0/5
C 11.11.11.0/24 [0/1] directly connected,   0/11
S 12.0.0.0/8 [5/0] directly connected, Null0
S 23.0.0.0/8 [3/0] directly connected, Null0
```

show ip route summary

Use this command to display the routing table summary. Use the optional *`all`* parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

Format	**`show ip route summary`** *`[all]`*
Modes	• Privileged EXEC • User EXEC

Term	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
RIP Routes	Total number of routes installed by RIP protocol.
OSPF Routes	Total number of routes installed by OSPF protocol.

Term	Definition
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	Total number of routes in the routing table.

The following shows example CLI display output for the command.

```
(Switch) #show ip route summary

Connected Routes..............................1
Static Routes.................................7
RIP Routes....................................0
BGP Routes....................................0
OSPF Routes...................................0
  Intra Area Routes...........................0
  Inter Area Routes...........................0
  External Type-1 Routes......................0
  External Type-2 Routes......................0
Reject Routes.................................2
Total routes..................................8
```

show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values. A route with a preference of 255 cannot be used to forward traffic.

Format	`show ip route preferences`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Local	The local route preference value.
Static	The static route preference value.
OSPF Intra	The OSPF Intra route preference value.
OSPF Inter	The OSPF Inter route preference value.
OSPF External	The OSPF External route preference value.
RIP	The RIP route preference value.

show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format	`show ip stats`
Modes	• Privileged EXEC • User EXEC

Virtual LAN Routing Commands

This section describes the commands you use to view and configure VLAN routing and to view VLAN routing status information.

vlan routing

This command enables routing on a VLAN. The vlanid value has a range from 1 to 4093. The [interface ID] value has a range from 1 to 128. Typically, you will not supply the interface ID argument, and the system automatically selects the interface ID. However, if you specify an interface ID that is already in use, the CLI displays an error message and does not create the VLAN interface..

Format	**`vlan routing`** *`<vlanid> [interface ID]`*
Mode	VLAN Config

no vlan routing

This command deletes routing on a VLAN. The *`<vlanid>`* value has a range from 1 to 4093.

Format	**`no vlan routing`** *`<vlanid>`*
Mode	VLAN Config

show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled.

Format	`show ip vlan`
Modes	• Privileged EXEC • User EXEC

Term	Definition
MAC Address used by Routing VLANs	The MAC Address associated with the internal bridge-router interface (IBRI). The same MAC Address is used by all VLAN routing interfaces. It will be displayed above the per-VLAN information.
VLAN ID	The identifier of the VLAN.
Logical Interface	The logical unit/slot/port associated with the VLAN routing interface.
IP Address	The IP address associated with this VLAN.
Subnet Mask	The subnet mask that is associated with this VLAN.

DHCP and BOOTP Relay Commands

This section describes the commands you use to configure BootP/DHCP Relay on the switch. A DHCP relay agent operates at Layer 3 and forwards DHCP requests and replies between clients and servers when they are not on the same physical subnet.

bootpdhcprelay cidoptmode

This command enables the circuit ID option mode for BootP/DHCP Relay on the system.

Default	disabled
Format	`bootpdhcprelay cidoptmode`
Mode	Global Config

no bootpdhcprelay cidoptmode

This command disables the circuit ID option mode for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay cidoptmode`
Mode	Global Config

bootpdhcprelay maxhopcount

This command configures the maximum allowable relay agent hops for BootP/DHCP Relay on the system. The *<hops>* parameter has a range of 1 to 16.

Default	4
Format	**`bootpdhcprelay maxhopcount`** *<1-16>*
Mode	Global Config

no bootpdhcprelay maxhopcount

This command configures the default maximum allowable relay agent hops for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay maxhopcount`
Mode	Global Config

bootpdhcprelay minwaittime

This command configures the minimum wait time in seconds for BootP/DHCP Relay on the system. When the BOOTP relay agent receives a BOOTREQUEST message, it MAY use the seconds-since-client-began-booting field of the request as a factor in deciding whether to relay the request or not. The parameter has a range of 0 to 100 seconds.

Default	0
Format	**`bootpdhcprelay minwaittime`** *<0-100>*
Mode	Global Config

no bootpdhcprelay minwaittime

This command configures the default minimum wait time in seconds for BootP/DHCP Relay on the system.

Format	`no bootpdhcprelay minwaittime`
Mode	Global Config

show bootpdhcprelay

This command displays the BootP/DHCP Relay information.

Format	`show bootpdhcprelay`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Maximum Hop Count	The maximum allowable relay agent hops.
Minimum Wait Time (Seconds)	The minimum wait time.
Admin Mode	Indicates whether relaying of requests is enabled or disabled.
Server IP Address	The IP address for the BootP/DHCP Relay server.
Circuit Id Option Mode	The DHCP circuit Id option which may be enabled or disabled.
Requests Received	The number or requests received.
Requests Relayed	The number of requests relayed.
Packets Discarded	The number of packets discarded.

IP Helper Commands

This section describes the commands to configure a DHCP relay agent with multiple DHCP server addresses per routing interface, and to use different server addresses for client packets arriving on different interfaces on the relay agent.

ip helper-address (Global Config)

Use the Global Configuration **ip helper-address** command to have the switch forward User Datagram Protocol (UDP) broadcasts received on an interface. To disable the forwarding of broadcast packets to specific addresses, use the no form of this command.

The **ip helper-address** command forwards specific UDP broadcast from one interface to another. You can define many helper addresses but the total number of address-port pairs is limited to 128 for the whole device. The setting of a helper address for a specific interface has precedence over a setting of a helper address for all interfaces. You cannot enable forwarding of BOOTP/DHCP packets (ports 67,68) with this command. If you want to relay BOOTP/DHCP packets, use the DHCP relay commands.

Ip-address: Destination broadcast or host address to be used when forwarding UDP broadcasts. You can specify 0.0.0.0 to indicate not to forward the UDP packet to any host and use "255.255.255.255" to broadcast the UDP packets to all hosts on the target subnet.

udp-port-list: The broadcast packet destination UDP port number to forward. If not specified, packets for the default services are forwarded to the helper address. Valid range, 0-65535.

Default	Disabled

Format	`ip helper-address <ip-address>`
	`{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|`
	`netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}`

Mode	Global Config

no ip helper-address (Global Config)

Use this command to remove the IP address from the previously configured list. The no command without an `<ip-address>` argument removes the entire list of helper addresses on that interface.

Format

```
no ip helper-address {<ip-address>}
{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
```

Mode GlobalConfig

ip helper-address

Use this command to add a unicast helper address to the list of helper addresses on an interface. This is the address of a DHCP server. This command can be applied multiple times on the routing interface to form the helper addresses list until the list reaches the maximum supported helper addresses.

Format

```
ip helper-address <ip-address>
{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
```

Mode Interface Config

no ip helper-address

Use this command to remove the IP address from the previously configured list. The no command without an `<ip-address>` argument removes the entire list of helper addresses on that interface.

Format

```
no ip helper-address {<ip-address>}
{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
```

Mode Interface Config

ip helper-address discard

Use this command to drop matching packets.

Format

```
ip helper-address discard
{<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|
netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}
```

Mode Interface Config

no ip helper-address discard

Use this command to permit the matching packets.

Format	`no ip helper-address discard {<1-65535>|dhcp|domain|isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|ntp|pim-auto-rip|rip|tacacs|tftp|time}`
Mode	Interface Config

show ip helper-address

Use this command to display the configured helper addresses on the given interface.

Format	`show ip helper-address <interface>`
Mode	• Privileged EXEC • User EXEC

The following shows example CLI display output for the command.

```
(switch) #show ip helper-address 1/0/1

Helper IP Address.............................. 1.2.3.4
............................................... 1.2.3.5
```

ICMP Throttling Commands

This section describes the commands you use to configure options for the transmission of various types of ICMP messages.

ip unreachables

Use this command to enable the generation of ICMP Destination Unreachable messages. By default, the generation of ICMP Destination Unreachable messages is enabled.

Default	enable
Format	`ip unreachables`
Mode	Interface Config

no ip unreachables

Use this command to prevent the generation of ICMP Destination Unreachable messages.

Format	`no ip unreachables`
Mode	Interface Config

ip redirects

Use this command to enable the generation of ICMP Redirect messages by the router. By default, the generation of ICMP Redirect messages is enabled.

Default	enable
Format	`ip redirects`
Mode	• Global Config • Interface Config

no ip redirects

Use this command to prevent the generation of ICMP Redirect messages by the router.

Format	`no ip redirects`
Mode	• Global Config • Interface Config

ip icmp echo-reply

Use this command to enable the generation of ICMP Echo Reply messages by the router. By default, the generation of ICMP Echo Reply messages is enabled.

Default	enable
Format	`ip icmp echo-reply`
Mode	Global Config

no ip icmp echo-reply

Use this command to prevent the generation of ICMP Echo Reply messages by the router.

Format	`no ip icmp echo-reply`
Mode	Global Config

ip icmp error-interval

Use this command to limit the rate at which IPv4 ICMP error messages are sent. The rate limit is configured as a token bucket, with two configurable parameters, *burst-size* and *burst-interval*.

The *burst-interval* specifies how often the token bucket is initialized with *burst-size* tokens. *burst-interval* is from 0 to 2147483647 milliseconds (msec).

The *burst-size* is the number of ICMP error messages that can be sent during one *burst-interval*. The range is from 1 to 200 messages.

To disable ICMP rate limiting, set *burst-interval* to zero (0).

Default	• *burst-interval* of 1000 msec. • *burst-size* of 100 messages
Format	`ip icmp error-interval` *<burst-interval> [<burst-size>]*
Mode	Global Config

no ip icmp error-interval

Use the **no** form of the command to return *burst-interval* and *burst-size* to their default values.

Format	`no ip icmp error-interval`
Mode	Global Config

Chapter 5
Quality of Service (QoS) Commands

This chapter describes the Quality of Service (QoS) commands available in the managed switch CLI.

The QoS Commands chapter contains the following sections:

> **Note:** The commands in this chapter are in one of two functional groups:
>
> - Show commands display switch settings, statistics, and other information.
> - Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.

Class of Service (CoS) Commands

This section describes the commands you use to configure and view Class of Service (CoS) settings for the switch. The commands in this section allow you to control the priority and transmission rate of traffic.

Note: Commands you issue in the Interface Config mode only affect a single interface. Commands you issue in the Global Config mode affect all interfaces.

classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class. The `<userpriority>` values can range from 0-7. The `<trafficclass>` values range from 0-6, although the actual number of available traffic classes depends on the platform. For more information about 802.1p priority, see "Voice VLAN Commands" on page 3-50.

Format	**classofservice dot1p-mapping** *<userpriority> <trafficclass>*
Modes	• Global Config • Interface Config

no classofservice dot1p-mapping

This command maps each 802.1p priority to its default internal traffic class value.

Format	`no classofservice dot1p-mapping`
Modes	• Global Config • Interface Config

classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The `<ipdscp>` value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

The `<trafficclass>` values can range from 0-6, although the actual number of available traffic classes depends on the platform.

Format	**`classofservice ip-dscp-mapping`** *`<ipdscp> <trafficclass>`*
Mode	Global Config

no classofservice ip-dscp-mapping

This command maps each IP DSCP value to its default internal traffic class value.

Format	`no classofservice ip-dscp-mapping`
Mode	Global Config

classofservice trust

This command sets the class of service trust mode of an interface. You can set the mode to trust one of the Dot1p (802.1p), IP DSCP, or IP Precedence packet markings. You can also set the interface mode to untrusted. If you configure an interface to use Dot1p, the mode does not appear in the output of the **`show running config`** command because Dot1p is the default.

> **Note:** The classofservice trust dot1p command will not be supported in future releases of the software because Dot1p is the default value. Use the no classofservice trust command to set the mode to the default value.

Default	dot1p
Format	**`classofservice trust`** *`{dot1p	ip-dscp	ip-precedence	untrusted}`*
Modes	• Global Config • Interface Config

no classofservice trust

This command sets the interface mode to the default value.

Format	`no classofservice trust`
Modes	• Global Config • Interface Config

cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The total number of queues supported per interface is platform specific. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format	**`cos-queue min-bandwidth`** *`<bw-0> <bw-1> … <bw-n>`*
Modes	• Global Config • Interface Config

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format	`no cos-queue min-bandwidth`
Modes	• Global Config • Interface Config

cos-queue strict

This command activates the strict priority scheduler mode for each specified queue.

Format	**`cos-queue strict`** *`<queue-id-1> [<queue-id-2> … <queue-id-n>]`*
Modes	• Global Config • Interface Config

no cos-queue strict

This command restores the default weighted scheduler mode for each specified queue.

Format	**`no cos-queue strict`** *`<queue-id-1> [<queue-id-2> … <queue-id-n>]`*
Modes	• Global Config • Interface Config

cos-queue random-detect

This command activates weighted random early discard (WRED) for each specified queue on the interface. Specific WRED parameters are configured using the randomdetect queue-parms and the random-detect exponential-weighting-constant commands. When specified in Interface Config' mode, this command affects a single interface only, whereas in Global Config mode, it applies to all interfaces. At least one, but no more than n, queue-id values are specified with this command.

Duplicate queue-id values are ignored. Each queue-id value ranges from 0 to (n-1), where n is the total number of queues supported per interface. The number n is platform dependant and corresponds to the number of supported queues (traffic classes).

Format	*`cos-queue random-detect queue-id-1 [queue-id-2 … queue-id-n]`*

Modes	`Global Config`
	`Interface Config`

random-detect exponential weighting-constant

This command is used to configure the WRED decay exponent for a CoS queue interface.

Format	*`random-detect exponential-weighting-constant 0-15`*
Modes	`Interface Config`

random-detect queue-parms

This command is used to configure WRED parameters for each drop precedence level supported by a queue. It is used only when per-COS queue configuration is enabled (using the *cos-queue random-detect* command).

min-thresh is the minimum threshold the queue depth (as a percentage) where WRED starts marking and dropping traffic.

max-thresh is the maximum threshold is the queue depth (as a percentage) above which WRED marks / drops all traffic.

drop-probability is the percentage probability that WRED will mark/drop a packet, when the queue depth is at the maximum threshold. (The drop probability increases linearly from 0 just before the minimum threshold, to this value at the maximum threshold, then goes to 100% for larger queue depths). Each parameter is specified for each possible drop precedence ("color" of TCP traffic).

The last precedence applies to all non-TCP traffic. For example, in a 3-color system, four of each parameter specified: green TCP, yellow TCP, red TCP, and non-TCP, respectively.

Format	*`random-detect queue-parms queue-id-1 [queue-id-2 … queue-id-n] minthresh thresh-prec-1 … thresh-prec-n max-thresh thresh-prec-1 … threshprec-n drop-probability prob-prec-1 … prob-prec-n`*
Modes	• Global Config • Interface Config

no random-detect queue-parms

Use this command to set the WRED configuration back to the default.

Format	*`no random-detect queue-parms queue-id-1 [queue-id-2 … queue-id-n]`*
Modes	• Global Config • Interface Config

traffic-shape

This command specifies the maximum transmission bandwidth limit for the interface as a whole. Also known as rate shaping, traffic shaping has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded.

Format	**`traffic-shape`** *`<bw>`*
Modes	• Global Config • Interface Config

no traffic-shape

This command restores the interface shaping rate to the default value.

Format	`no traffic-shape`
Modes	• Global Config • Interface Config

show classofservice dot1p-mapping

This command displays the current Dot1p (802.1p) priority mapping to internal traffic classes for a specific interface. The *<unit/slot/port>* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the 802.1p mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed. For more information, see "Voice VLAN Commands" on page 3-50.

Format	**show classofservice dot1p-mapping** *[<unit/slot/port>]*
Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
User Priority	The 802.1p user priority value.
Traffic Class	The traffic class internal queue identifier to which the user priority value is mapped.

show classofservice ip-precedence-mapping

This command displays the current IP Precedence mapping to internal traffic classes for a specific interface. The unit/slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the IP Precedence mapping table of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format	**show classofservice ip-precedence-mapping** *[<unit/slot/port>]*
Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP Precedence	The IP Precedence value.
Traffic Class	The traffic class internal queue identifier to which the IP Precedence value is mapped.

show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format	`show classofservice ip-dscp-mapping`
Mode	Privileged EXEC

The following information is repeated for each user priority.

Term	Definition
IP DSCP	The IP DSCP value.
Traffic Class	The traffic class internal queue identifier to which the IP DSCP value is mapped.

show classofservice trust

This command displays the current trust mode setting for a specific interface. The *`<unit/slot/port>`* parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If you specify an interface, the command displays the port trust mode of the interface. If you do not specify an interface, the command displays the most recent global configuration settings.

Format	**`show classofservice trust`** *`[<unit/slot/port>]`*
Mode	Privileged EXEC

Term	Definition
Non-IP Traffic Class	The traffic class used for non-IP traffic. This is only displayed when the COS trust mode is set to trust IP Precedence or IP DSCP (on platforms that support IP DSCP).
Untrusted Traffic Class	The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The unit/slot/port parameter is optional and is only valid on platforms that support independent per-port class of service mappings. If specified, the class-of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format	**`show interfaces cos-queue`** *[<unit/slot/port>]*
Mode	Privileged EXEC

Term	Definition
Queue Id	An interface supports n queues numbered 0 to (n-1). The specific n value is platform dependent.
Minimum Bandwidth	The minimum transmission bandwidth guarantee for the queue, expressed as a percentage. A value of 0 means bandwidth is not guaranteed and the queue operates using best-effort. This is a configured value.
Scheduler Type	Indicates whether this queue is scheduled for transmission using a strict priority or a weighted scheme. This is a configured value.
Queue Management Type	The queue depth management technique used for this queue (tail drop).

If you specify the interface, the command also displays the following information.

Term	Definition
Interface	The unit/slot/port of the interface. If displaying the global configuration, this output line is replaced with a Global Config indication.
Interface Shaping Rate	The maximum transmission bandwidth limit for the interface as a whole. It is independent of any per-queue maximum bandwidth value(s) in effect for the interface. This is a configured value.

Differentiated Services (DiffServ) Commands

This section describes the commands you use to configure QOS Differentiated Services (DiffServ).

You configure DiffServ in several stages by specifying three DiffServ components:

1. Class

   a. Creating and deleting classes.

   b. Defining match criteria for a class.

2. Policy

   a. Creating and deleting policies

   b. Associating classes with a policy

   c. Defining policy statements for a policy/class combination

3. Service

   a. Adding and removing a policy to/from an inbound interface

The DiffServ class defines the packet filtering criteria. The attributes of a DiffServ policy define the way the switch processes packets. You can define policy attributes on a per-class instance basis. The switch applies these attributes when a match occurs.

Packet processing begins when the switch tests the match criteria for a packet. The switch applies a policy to a packet when it finds a class match within that policy.

The following rules apply when you create a DiffServ class:

- Each class can contain a maximum of one referenced (nested) class
- Class definitions do not support hierarchical service policies

A given class definition can contain a maximum of one reference to another class. You can combine the reference with other match criteria. The referenced class is truly a reference and not a copy since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes, otherwise the switch rejects the change. You can remove a class reference from a class definition.

The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

Note: The mark possibilities for policing include CoS, IP DSCP, and IP Precedence. While the latter two are only meaningful for IP packet types, CoS marking is allowed for both IP and non-IP packets, since it updates the 802.1p user priority field contained in the VLAN tag of the layer 2 packet header.

diffserv

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`diffserv`
Mode	Global Config

no diffserv

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, DiffServ services are activated.

Format	`no diffserv`
Mode	Global Config

DiffServ Class Commands

Use the DiffServ class commands to define traffic classification. To classify traffic, you specify Behavior Aggregate (BA), based on DSCP and Multi-Field (MF) classes of traffic (name, match criteria)

This set of commands consists of class creation/deletion and matching, with the class match commands specifying Layer 3, Layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic that belongs to the class.

Note: Once you create a class match criterion for a class, you cannot change or delete the criterion. To change or delete a class match criterion, you must delete and re-create the entire class.

The CLI command root is **`class-map`**.

class-map

This command defines a DiffServ class of type match-all. When used without any match condition, this command enters the class-map mode. The `<class-map-name>` is a case sensitive alphanumeric string from 1 to 31 characters uniquely identifying an existing DiffServ class.

Note: The class-map-name 'default' is reserved and must not be used.

The class type of **`match-all`** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.This command may be used without specifying a class type to enter the Class-Map Config mode for an existing DiffServ class.

Note: The optional keywords `[{ipv4 | ipv6}]` specify the Layer 3 protocol for this class. If not specified, this parameter defaults to `‘ipv4’`. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

Note: The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the `[{ipv4 | ipv6}]` keyword specified.

Format	**`class-map match-all`** *`<class-map-name>`* `[{ipv4	ipv6}]`
Mode	Global Config

no class-map

This command eliminates an existing DiffServ class. The `<class-map-name>` is the name of an existing DiffServ class. (The class name ‘default’ is reserved and is not allowed here.) This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, the delete action fails.

Format	**`no class-map`** *`<class-map-name>`*
Mode	Global Config

class-map rename

This command changes the name of a DiffServ class. The *<class-map-name>* is the name of an existing DiffServ class. The *<new-class-map-name>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

Default	none
Format	**`class-map rename`** *`<class-map-name> <new-class-map-name>`*
Mode	Global Config

match ethertype

This command adds to the specified class definition a match condition based on the value of the ethertype. The *<ethertype>* value is specified as one of the following keywords: **appletalk**, **arp**, **ibmsna**, **ipv4**, **ipv6**, **ipx**, **mplsmcast**, **mplsucast**, **netbios**, **novell**, **pppoe**, **rarp** or as a custom ethertype value in the range of 0x0600-0xFFFF.

Format	**`match ethertype`** *`{<keyword> | custom <0x0600-0xFFFF>}`*
Mode	Class-Map Config Ipv6-Class-Map Config

match any

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Default	none
Format	`match any`
Mode	Class-Map Config Ipv6-Class-Map Config

match class-map

This command adds to the specified class definition the set of match conditions defined for another class. The *<refclassname>* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Default	none
Format	`match class-map` *<refclassname>*
Mode	Class-Map Config Ipv6-Class-Map Config

Note:
- The parameters *<refclassname>* and *<class-map-name>* can not be the same.
- Only one other class may be referenced by a class.
- Any attempts to delete the *<refclassname>* class while the class is still referenced by any *<class-map-name>* fails.
- The combined match criteria of *<class-map-name>* and *<refclassname>* must be an allowed combination based on the class type.
- Any subsequent changes to the *<refclassname>* class match criteria must maintain this validity, or the change attempt fails.
- The total number of class rules formed by the complete reference class chain (including both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

no match class-map

This command removes from the specified class definition the set of match conditions defined for another class. The *<refclassname>* is the name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

Format	`no match class-map` *<refclassname>*
Mode	Class-Map Config Ipv6-Class-Map Config

match cos

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

Default	none
Format	**`match cos`** *`<0-7>`*
Mode	Class-Map Config Ipv6-Class-Map Config

match ip6flowlbl

This command adds to the specified class definition a match condition based on the IP6flowlbl of a packet. The `label` is the value to match in the Flow Label field of the IPv6 header (range 0-1048575).

Format	`match ip6flowlbl` *`<label>`*
Mode	Ipv6-Class-Map Configuration mode

match destination-address mac

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The `<macaddr>` parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The **`<macmask>`** parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Default	none
Format	**`match destination-address mac`** *`<macaddr> <macmask>`*
Mode	Class-Map Config Ipv6-Class-Map Config

match dstip

This command adds to the specified class definition a match condition based on the destination IP address of a packet. The *<ipaddr>* parameter specifies an IP address. The *<ipmask>* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	**`match dstip`** *`<ipaddr> <ipmask>`*
Mode	Class-Map Config

match dstip6

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Default	none
Format	**`match dstip6`** *`<destination-ipv6-prefix/prefix-length>`*
Mode	Ipv6-Class-Map Config

match dstl4port

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword, the value for *<portkey>* is one of the supported port name keywords. The currently supported *<portkey>* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number. To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default	none
Format	**`match dstl4port`** *`{<portkey>	<0-65535>}`*
Mode	Class-Map Config Ipv6-Class-Map Config

match ip dscp

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

The *<dscpval>* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Note: The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	**`match ip dscp`** *`<dscpval>`*
Mode	Class-Map Config Ipv6-Class-Map Config

match ip precedence

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7.

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Default	none
Format	**`match ip precedence`** *`<0-7>`*
Mode	Class-Map Config

match ip tos

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header. The value of `<tosbits>` is a two-digit hexadecimal number from 00 to ff. The value of `<tosmask>` is a two-digit hexadecimal number from 00 to ff. The `<tosmask>` denotes the bit positions in `<tosbits>` that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a `<tosbits>` value of a0 (hex) and a `<tosmask>` of a2 (hex).

Note: The IP DSCP, IP Precedence, and IP ToS match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

Note: This "free form" version of the IP DSCP/Precedence/TOS match specification gives the user complete control when specifying which bits of the IP Service Type field are checked.

Default	none
Format	**`match ip tos`** *`<tosbits> <tosmask>`*
Mode	Class-Map Config

match protocol

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

To specify the match condition using a single keyword notation, the value for `<protocol-name>` is one of the supported protocol name keywords. The currently supported values are: *`icmp`*, *`igmp`*, *`ip`*, *`tcp`*, *`udp`*. A value of *`ip`* matches all protocol number values.

To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

Note: This command does not validate the protocol number value against the current list defined by IANA.

Default	none
Format	**`match protocol`** *`{<protocol-name>	<0-255>}`*
Mode	Class-Map Config Ipv6-Class-Map Config

match source-address mac

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The `<address>` parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The `<macmask>` parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

Default	none
Format	**`match source-address mac`** *`<address> <macmask>`*
Mode	Class-Map Config Ipv6-Class-Map Config

match srcip

This command adds to the specified class definition a match condition based on the source IP address of a packet. The *`<ipaddr>`* parameter specifies an IP address. The *`<ipmask>`* parameter specifies an IP address bit mask and must consist of a contiguous set of leading 1 bits.

Default	none
Format	**`match srcip`** *`<ipaddr> <ipmask>`*
Mode	Class-Map Config

match srcip6

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Default	none
Format	**`match srci`**`p6 <source-ipv6-prefix/prefix-length>`
Mode	Ipv6-Class-Map Config

match srcl4port

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation. To specify the match condition as a single keyword notation, the value for *<portkey>* is one of the supported port name keywords (listed below). The currently supported *<portkey>* values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.

To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535.

Default	none
Format	**match srcl4port** *{<portkey> | <0-65535>}*
Mode	Class-Map Config Ipv6-Class-Map Config

DiffServ Policy Commands

Use the DiffServ policy commands to specify traffic conditioning actions, such as policing and marking, to apply to traffic classes

Use the policy commands to associate a traffic class that you define by using the class command set with one or more QoS policy attributes. Assign the class/policy association to an interface to form a service. Specify the policy name when you create the policy.

Each traffic class defines a particular treatment for packets that match the class definition. You can associate multiple traffic classes with a single policy. When a packet satisfies the conditions of more than one class, preference is based on the order in which you add the classes to the policy. The first class you add has the highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes.

Note: The only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is **policy-map**.

assign-queue

This command modifies the queue id to which the associated traffic stream is assigned. The `queueid` is an integer from 0 to *n*-1, where *n* is the number of egress queues supported by the device.

Format	**`assign-queue`** *`<queueid>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop

drop

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format	`drop`
Mode	Policy-Class-Map Config
Incompatibilities	Assign Queue, Mark (all forms), Mirror, Police, Redirect

mirror

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

Format	**`mirror`** *`<unit/slot/port>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Redirect

redirect

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Format	**`redirect`** *`<unit/slot/port>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mirror

conform-color

Use this command to enable color-aware traffic policing and define the conform-color class map. Used in conjunction with the police command where the fields for the conform level are specified. The `<class-map-name>` parameter is the name of an existing DiffServ class map.

Note: This command may only be used after specifying a police command for the policy-class instance.

Format	**`conform-color`** *`<class-map-name>`*
Mode	Policy-Class-Map Config

class

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements. The *`<classname>`* is the name of an existing DiffServ class.

Note: This command causes the specified policy to create a reference to the class definition.

Note: The CLI mode is changed to Policy-Class-Map Config when this command is successfully executed.

Format	**`class`** *`<classname>`*
Mode	Policy-Map Config

no class

This command deletes the instance of a particular class and its defined treatment from the specified policy. `<classname>` is the names of an existing DiffServ class.

Note: This command removes the reference to the class definition for the specified policy.

Format	**`no class`** *`<classname>`*
Mode	Policy-Map Config

mark cos

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.mark ip-dscp

Default	1
Format	**`mark-cos`** *`<0-7>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark IP DSCP, IP Precedence, Police

mark ip-dscp

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

The *`<dscpval>`* value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format	**`mark ip-dscp`** *`<dscpval>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police

mark ip-precedence

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Note: This command may not be used on IPv6 classes. IPv6 does not have a precedence field.

Format	**`mark ip-precedence`** *`<0-7>`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark CoS, Mark IP Precedence, Police
Policy Type	In

police-simple

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

For set-dscp-transmit, a *`<dscpval>`* value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format	**`police-simple`** *`{<1-4294967295> <1-128> conform-action {drop	set-prec-transmit <0-7>	set-dscp-transmit <0-63>	set-cos-transmit <0-7>	transmit} [violate-action {drop	set-prec-transmit <0-7>	set-dscp-transmit <0-63>	set-cos-transmit <0-7>	transmit}]}`*
Mode	Policy-Class-Map Config
Incompatibilities	Drop, Mark (all forms)

policy-map

This command establishes a new DiffServ policy. The `<policyname>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

Note: The CLI mode is changed to Policy-Map Config when this command is successfully executed.

Format	**`policy-map`** *`<policyname>`* **`in`**
Mode	Global Config

no policy-map

This command eliminates an existing DiffServ policy. The `<policyname>` parameter is the name of an existing DiffServ policy. This command may be issued at any time. If the policy is currently referenced by one or more interface service attachments, this delete attempt fails.

Format	**`no policy-map`** *`<policyname>`*
Mode	Global Config

policy-map rename

This command changes the name of a DiffServ policy. The `<policyname> i`s the name of an existing DiffServ class. The `<newpolicyname>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format	**`policy-map rename`** *`<policyname> <newpolicyname>`*
Mode	Global Config

DiffServ Service Commands

Use the DiffServ service commands to assign a DiffServ traffic conditioning policy, which you specified by using the policy commands, to an interface in the incoming direction

The service commands attach a defined policy to a directional interface. You can assign only one policy at any one time to an interface in the inbound direction. DiffServ is not used in the outbound direction.

This set of commands consists of service addition/removal.

The CLI command root is **`service-policy`**.

service-policy

This command attaches a policy to an interface in the inbound direction. The *`<policyname>`* parameter is the name of an existing DiffServ policy. This command causes a service to create a reference to the policy.

Note: This command effectively enables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Note: This command fails if any attributes within the policy definition exceed the capabilities of the interface. Once a policy is successfully attached to an interface, any attempt to change the policy definition, that would result in a violation of the interface capabilities, causes the policy change attempt to fail.

Format	**`service-policy in`** *`<policymapname>`*
Modes	• Global Config • Interface Config

Note: Each interface can have one policy attached.

no service-policy

This command detaches a policy from an interface in the inbound direction. The `<policyname>` parameter is the name of an existing DiffServ policy.

Note: This command causes a service to remove its reference to the policy. This command effectively disables DiffServ on an interface in the inbound direction. There is no separate interface administrative 'mode' command for DiffServ.

Format `no service-policy in <policymapname>`

Modes
- Global Config
- Interface Config

DiffServ Show Commands

Use the DiffServ show commands to display configuration and status information for classes, policies, and services. You can display DiffServ information in summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled.

show class-map

This command displays all configuration information for the specified class. The `<class-name>` is the name of an existing DiffServ class.

Format `show class-map <class-name>`

Modes
- Privileged EXEC
- User EXEC

If the class-name is specified the following fields are displayed:

Term	Definition
Class Name	The name of this class.
Class Type	A class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Class Layer3 Protocol	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.

Term	Definition
Match Criteria	The Match Criteria fields are only displayed if they have been configured. Not all platforms support all match criteria values. They are displayed in the order entered by the user. The fields are evaluated in accordance with the class type. The possible Match Criteria fields are: Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Ethertype, Source MAC Address, VLAN, Class of Service, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, and Source Layer 4 Port.
Values	The values of the Match Criteria.

If you do not specify the Class Name, this command displays a list of all defined DiffServ classes. The following fields are displayed:

Term	Definition
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	A class type of ‘all’ means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Reference Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

show diffserv

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables. This command takes no options.

Format	`show diffserv`
Mode	Privileged EXEC

Term	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current /Max	The current number of entries (rows) and the maximum allowed entries (rows) in the Class Table.
Class Rule Table Size Current /Max	The current number of entries (rows) and the maximum allowed entries (rows) in the Class Rule Table.

Term	Definition
Policy Table Size Current /Max	The current number of entries (rows) and the maximum allowed entries (rows) in the Policy Table.
Policy Instance Table Size Current /Max	Current number of entries (rows) and the maximum allowed entries (rows) in the Policy Instance Table.
Policy Attribute Table Size Current /Max	Current number of entries (rows) and the maximum allowed entries (rows) in the Policy Attribute Table.
Service Table Size Current /Max	The current number of entries (rows) i and the maximum allowed entries (rows) in the Service Table.

show policy-map

This command displays all configuration information for the specified policy. The `<policyname>` is the name of an existing DiffServ policy.

Format	**`show policy-map`** *`[policyname]`*
Mode	Privileged EXEC

If the Policy Name is specified the following fields are displayed:

Term	Definition
Policy Name	The name of this policy.
Policy Type	The policy type (Only inbound policy definitions are supported for this platform.)

The following information is repeated for each class associated with this policy (only those policy attributes actually configured are displayed):

Term	Definition
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Class Name	The name of this class.
Committed Burst Size (KB)	The committed burst size, used in simple policing.
Committed Rate (Kbps)	The committed rate, used in simple policing,
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.

Term	Definition
Conform COS	The CoS mark value if the conform action is set-cos-transmit.
Conform DSCP Value	The DSCP mark value if the conform action is set-dscp-transmit.
Conform IP Precedence Value	The IP Precedence mark value if the conform action is set-prec-transmit.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Mark CoS	The class of service value that is set in the 802.1p header of inbound packets. This is not displayed if the mark cos was not specified.
Mark IP DSCP	The mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified.
Mark IP Precedence	The mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if mark ip precedence is not specified.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform COS	The CoS mark value if the non-conform action is set-cos-transmit.
Non-Conform DSCP Value	The DSCP mark value if the non-conform action is set-dscp-transmit.
Non-Conform IP Precedence Value	The IP Precedence mark value if the non-conform action is set-prec-transmit.
Policing Style	The style of policing, if any, used (simple).
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.

If the Policy Name is not specified this command displays a list of all defined DiffServ policies. The following fields are displayed:

Term	Definition
Policy Name	The name of this policy. (The order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type (Only inbound is supported).

Term	Definition
Class Members	List of all class names associated with this policy.

show diffserv service

This command displays policy service information for the specified interface and direction. The *<unit/slot/port>* parameter specifies a valid unit/slot/port number for the system.

Format	**show diffserv service** *<unit/slot/port>* **in**
Mode	Privileged EXEC

Term	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	Valid slot and port number separated by forward slashes.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.
Policy Details	Attached policy details, whose content is identical to that described for the show policy-map *<policymapname>* command (content not repeated here for brevity).

show diffserv service brief

This command displays all interfaces in the system to which a DiffServ policy has been attached. The inbound direction parameter is optional.

Format	**show diffserv service brief** *[in]*
Mode	Privileged EXEC

Term	Definition
DiffServ Admin Mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

show policy-map interface

This command displays policy-oriented statistics information for the specified interface and direction. The `<unit/slot/port>` parameter specifies a valid interface for the system.

Note: This command is only allowed while the DiffServ administrative mode is enabled.

Format	**`show policy-map interface`** *`<unit/slot/port> [in]`*
Mode	Privileged EXEC

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Direction	The traffic direction of this interface service.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Term	Definition
Class Name	The name of this class instance.
In Discarded Packets	A count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

show service-policy

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction.

Format	`show service-policy in`
Mode	Privileged EXEC

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Term	Definition
Interface	Valid slot and port number separated by forward slashes.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

MAC Access Control List (ACL) Commands

This section describes the commands you use to configure MAC ACL settings. MAC ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to MAC ACLs:

- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per MAC ACL is hardware dependent.

mac access-list extended

This command creates a MAC Access Control List (ACL) identified by `<name>`, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The `<name>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

⇨	**Note:** The CLI mode changes to Mac-Access-List Config mode when you successfully execute this command.

Format	**`mac access-list extended`** *`<name>`*
Mode	Global Config

no mac access-list extended

This command deletes a MAC ACL identified by *`<name>`* from the system.

Format	**`no mac access-list extended`** *`<name>`*
Mode	Global Config

mac access-list extended rename

This command changes the name of a MAC Access Control List (ACL). The *`<name>`* parameter is the name of an existing MAC ACL. The *`<newname>`* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.

This command fails if a MAC ACL by the name *`<newname>`* already exists.

Format	**`mac access-list extended rename`** *`<name> <newname>`*
Mode	Global Config

{deny | permit} (MAC ACL)

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

⇨	**Note:** The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

Note: An implicit 'deny all' MAC rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported *<ethertypekey>* values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138
pppoe	0x8863, 0x8864
rarp	0x8035

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed `<queue-id>` value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a **`permit`** rule.

Note: The special command form {deny | permit} any any is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list "match every" rule.

Format	`{deny|permit} {<srcmac>	any} {<dstmac>	any} [<ethertypekey>	<0x0600-0xFFFF>] [vlan {eq <0-4095>}] [cos <0-7>] [[log] [assign-queue <queue-id>]] [{mirror	redirect} <unit/slot/port>]`
Mode	Mac-Access-List Config

mac access-group

This command either attaches a specific MAC Access Control List (ACL) identified by *`<name>`* to an interface, or associates it with a VLAN ID, in a given direction. The *`<name>`* parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other mac access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified mac access list replaces the currently attached mac access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: You should be aware that the <`out`> option may or may not be available, depending on the platform.

Format	**mac access-group** *<name> [vlan <vlan-id>]* **[in|out]** *[sequence <1-4294967295>]*
Modes	• Global Config • Interface Config

no mac access-group

This command removes a MAC ACL identified by *<name>* from the interface in a given direction.

Format	**no mac access-group** *<name> [vlan <vlan-id>]* **in**
Modes	• Global Config • Interface Config

show mac access-lists

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. Use the *[name]* parameter to identify a specific MAC ACL to display.

Format	**show mac access-lists** *[name]*
Mode	Privileged EXEC

Term	Definition
Rule Number	The ordered rule number identifier defined within the MAC ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	The source MAC address for this rule.
Destination MAC Address	The destination MAC address for this rule.
Ethertype	The Ethertype keyword or custom value for this rule.
VLAN ID	The VLAN identifier value or range for this rule.
COS	The COS (802.1p) value for this rule.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.

Term	Definition
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.

IP Access Control List (ACL) Commands

This section describes the commands you use to configure IP ACL settings. IP ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IP ACLs:

- Managed switch software does not support IP ACL configuration for IP packet fragments.
- The maximum number of ACLs you can create is hardware dependent. The limit applies to all ACLs, regardless of type.
- The maximum number of rules per IP ACL is hardware dependent.
- Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0’s) in a bit position that must be checked. A ‘1’ in a bit position of the ACL mask indicates the corresponding bit can be ignored.

access-list

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs.

IP Standard ACL:

Format	**`access-list`** *`<1-99> {deny	permit} {every	<srcip> <srcmask>} [log] [assign-queue <queue-id>] [{mirror	redirect} <unit/slot/port>]`*
Mode	Global Config

IP Extended ACL:

Format	**`access-list`** *`<100-199> {deny	permit} {every	{{icmp	igmp	ip	tcp	udp	<number>} <srcip> <srcmask>[{eq {<portkey>	<0-65535>} <dstip> <dstmask> [{eq {<portkey>| <0-65535>}] [precedence <precedence>	tos <tos> <tosmask>	dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror	redirect} <unit/slot/port>]`*
Mode	Global Config

Parameter	Description
`<1-99> or <100-199>`	Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
`{deny | permit}`	Specifies whether the IP ACL rule permits or denies an action.
`every`	Match every packet
`{icmp | igmp | ip | tcp | udp | <number>}`	Specifies the protocol to filter for an extended IP ACL rule.
`<srcip> <srcmask>`	Specifies a source IP address and source netmask for match condition of the IP ACL rule.
`[{eq {<portkey> | <0-65535>}]`	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number, which ranges from 0-65535, or you specify the <*`portkey`*>, which can be one of the following keywords: *`domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp`*, and *www*. Each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range.
`<dstip> <dstmask>`	Specifies a destination IP address and netmask for match condition of the IP ACL rule.
`[precedence <precedence> | tos <tos> <tosmask> | dscp <dscp>]`	Specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *`dscp`*, *`precedence`*, *`tos/tosmask`*.
`[log]`	Specifies that this rule is to be logged.
`[assign-queue <queue-id>]`	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned.
`[{mirror | redirect} <unit/slot/port>]`	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.

no access-list

This command deletes an IP ACL that is identified by the parameter *`<accesslistnumber>`* from the system. The range for *`<accesslistnumber>`* 1-99 for standard access lists and 100-199 for extended access lists.

Format	**`no access-list`** *`<accesslistnumber>`*
Mode	Global Config

ip access-list

This command creates an extended IP Access Control List (ACL) identified by <*name*>, consisting of classification fields defined for the IP header of an IPv4 frame. The <*name*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

➡	**Note:** The CLI mode changes to IPv4-Access-List Config mode when you successfully execute this command.

Format	**`ip access-list`** *`<name>`*
Mode	Global Config

no ip access-list

This command deletes the IP ACL identified by <name> from the system.

Format	**`no ip access-list`** *`<name>`*
Mode	Global Config

ip access-list rename

This command changes the name of an IP Access Control List (ACL). The <*name*> parameter is the names of an existing IP ACL. The <new*name*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

This command fails is an IP ACL by the name <new*name*> already exists.

Format	**`ip access-list rename`** *`<name> <newname>`*
Mode	Global Config

{deny | permit} (IP ACL)

This command creates a new rule for the current IP access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within an IP ACL cannot be deleted individually. Rather, the entire IP ACL must be deleted and re-specified.

Note: An implicit 'deny all' IP rule always terminates the access list.

Note: For the XSM7224S, the *`mirror`* parameter allows the traffic matching this rule to be copied to the specified *`<unit/slot/port>`*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *`<unit/slot/port>`*. The *`assign-queue`* and *`redirect`* parameters are only valid for a `permit` rule.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the every keyword or the protocol, source address, and destination address values must be specified. The source and destination IP address fields may be specified using the keyword ‘`any`’ to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed `<queue-id>` value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a **`permit`** rule.

Format

```
{deny | permit} {every | {{icmp | igmp | ip | tcp | udp | <number>}
<srcip> <srcmask>[{eq {<portkey> | <0-65535>} <dstip> <dstmask> [{eq
{<portkey>| <0-65535>}] [precedence <precedence> | tos <tos> <tosmask>
| dscp <dscp>] [log] [assign-queue <queue-id>] [{mirror | redirect}
<unit/slot/port>]
```

Mode Ipv4-Access-List Config

ip access-group

This command either attaches a specific IP ACL identified by `<accesslistnumber>` to an interface or associates with a VLAN ID in a given direction. The parameter `<name>` is the name of the Access Control List.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Note: You should be aware that the <`out`> option may or may not be available, depending on the platform.

Default none

Format

```
ip access-group <accesslistnumber> <name> [vlan <vlan-id>] <in |
out>[sequence <1-4294967295>]
```

Modes

- Interface Config
- Global Config

no ip access-group

This command removes a specified IP ACL from an interface.

Default	none
Format	**no ip access-group** *<accesslistnumber> [vlan <vlan-id>]* **in**
Mode	• Interface Config • Global Config

acl-trapflags

This command enables the ACL trap mode.

Default	disabled
Format	acl-trapflags
Mode	Global Config

no acl-trapflags

This command disables the ACL trap mode.

Format	no acl-trapflags
Mode	Global Config

show ip access-lists

This command displays an IP ACL *<accesslistnumber>* is the number used to identify the IP ACL.

Format	**show ip access-lists** *<accesslistnumber>*
Mode	Privileged EXEC

Note: Only the access list fields that you configure are displayed.

Term	Definition
Rule Number	The number identifier for each rule that is defined for the IP ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source IP Mask	The source IP Mask for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination IP Mask	The destination IP Mask for this rule.
Destination L4 Port Keyword	The destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified IP Precedence.
IP TOS	The value specified for IP TOS.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.

show access-lists

This command displays IP ACLs, IPv6 ACLs, and MAC access control lists information for a designated interface and direction.

Format	**`show access-lists interface`** *`<unit/slot/port>`* **`in`**
Mode	Privileged EXEC

Term	Definition
ACL Type	Type of access list (IP, IPv6, or MAC).

Term	Definition
ACL ID	Access List name for a MAC or IPv6 access list or the numeric identifier for an IP access list.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

IPv6 Access Control List (ACL) Commands

This section describes the commands you use to configure IPv6 ACL settings. IPv6 ACLs ensure that only authorized users have access to specific resources and block any unwarranted attempts to reach network resources.

The following rules apply to IPv6 ACLs:

- The maximum number of ACLs you create is 100, regardless of type.
- The system supports only Ethernet II frame types.
- The maximum number of rules per IPv6 ACL is hardware dependent.

ipv6 access-list

This command creates an IPv6 Access Control List (ACL) identified by `<name>`, consisting of classification fields defined for the IP header of an IPv6 frame. The `<name>` parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

Note: The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

Format **`ipv6 access-list`** *<name>*

Mode Global Config

no ipv6 access-list

This command deletes the IPv6 ACL identified by *<name>* from the system.

Format	`no ipv6 access-list <name>`
Mode	Global Config

ipv6 access-list rename

This command changes the name of an IPv6 ACL. The *<name>* parameter is the name of an existing IPv6 ACL. The *<newname>* parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name *<newname>* already exists.

Format	**`ipv6 access-list rename`** `<name> <newname>`
Mode	Global Config

{deny | permit} (IPv6)

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

Note: The ‘no’ form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

Note: An implicit ‘deny all’ IPv6 rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the *‘every’* keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword *‘any’* to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed *`<queue-id>`* value is 0-(n-1), where *`n`* is the number of user configurable queues available for the hardware platform. The *`assign-queue`* parameter is valid only for a permit rule.

The *`mirror`* parameter allows the traffic matching this rule to be copied to the specified *`<unit/slot/port>`*, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified *`<unit/slot/port>`*. The *`assign-queue`* and *`redirect`* parameters are only valid for a **`permit`** rule.

Format	`{deny	permit} {every	{{icmp	igmp	ipv6	tcp	udp	<number>}[log] [assign-queue <queue-id>] [{mirror	redirect} <unit/slot/port>]`
Mode	IPv6-Access-List Config

ipv6 traffic-filter

This command either attaches a specific IPv6 ACL identified by `<name>` to an interface or associates with a VLAN ID in a given direction. The <name> parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The `vlan` keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

Note: You should be aware that the <`out`> option may or may not be available, depending on the platform.

Format	**`ipv6 traffic-filter <name>`** *`[vlan <vlan-id>]`* **`<in	out>`***`[sequence <1-4294967295>]`*
Modes	• Global Config • Interface Config

no ipv6 traffic-filter

This command removes an IPv6 ACL identified by `<name>` from the interface(s) in a given direction.

Format	**`no ipv6 traffic-filter <name>`** *`[vlan <vlan-id>]`* **`in`** *`[sequence <1-4294967295>]`*
Modes	• Global Config • Interface Config

show ipv6 access-lists

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the `[name]` parameter to identify a specific IPv6 ACL to display.

Format	**`show ipv6 access-lists`** *`[name]`*
Mode	Privileged EXEC

Term	Definition
Rule Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match All	Indicates whether this access list applies to every packet. Possible values are True or False.
Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.

Term	Definition
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The unit/slot/port to which packets matching this rule are copied.
Redirect Interface	The unit/slot/port to which packets matching this rule are forwarded.

Auto-Voice over IP Commands

This section describes the commands you use to configure Auto-Voice over IP (VoIP) commands. The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class-of-service than ordinary traffic. When you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected, the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

auto-voip all

Use this command to enable VoIP Profile on the interfaces of the switch.

Default	disabled
Format	`auto-voip all`
Mode	Global Config

no auto-voip all

Use this command to disable VoIP Profile on the interfaces of the switch.

Format	`no auto-voip all`
Mode	Global Config

auto-voip

Use this command to enable VoIP Profile on the interface.

Default	disabled
Format	`auto-voip`
Mode	Interface Config

no auto-voip

Use this command to disable VoIP Profile on the interface.

Format	`no auto-voip all`
Mode	Interface Config

show auto-voip

Use this command to display the VoIP Profile settings on the interface or interfaces of the switch.

Format	`show auto-voip interface {<unit/slot/port>|all}`
Mode	Privileged EXEC

Field	Description
AutoVoIP Mode	The Auto VoIP mode on the interface.
Traffic Class	The CoS Queue or Traffic Class to which all VoIP traffic is mapped to. This is not configurable and defaults to the highest CoS queue available in the system for data traffic.

Chapter 6
Utility Commands

This chapter describes the utility commands available in the CLI.

The Utility Commands chapter includes the following sections:

Note: The commands in this chapter are in one of four functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear some or all of the settings to factory defaults.

Auto Install Commands

This section describes the Auto Install Commands. Auto Install is a software feature which provides for the configuration of a switch automatically when the device is initialized and no configuration file is found on the switch. The Auto Install process requires DHCP to be enabled by default in order for it to be completed. The downloaded config file is not automatically saved to startup-config. An administrator must explicitly issue a save request in order to save the configuration. The Auto Install process depends upon the configuration of other devices in the network, including a DHCP or BOOTP server, a TFTP server and, if necessary, a DNS server.

There are three steps to Auto Install:

1. Configuration or assignment of an IP address for the device.
2. Assignment of a TFTP server.
3. Obtain a configuration file for the device from the TFTP server.

show autoinstall

This command displays the current status of the Auto Config process.

Format	`show autoinstall`
Mode	Privileged EXEC

Term	Definition
AutoInstall Mode	The administrator mode is enabled or disabled.
AutoSave Modet	If this option is enabled, the downloaded config file will be saved. Otherwise, administrator must explicitly issue a "copy running-config startup-config" command in order to save the configuration.
AutoInstall Retry Count	the number of attempts to download a configuration.
AutoInstall State	The status of the AutoInstall.

Example

```
(switch) #show autoinstall
AutoInstall Mode.............................. Stopped
AutoSave Mode................................. Disabled
AutoInstall Retry Count....................... 3
AutoInstall State............................. Waiting for boot options
```

boot autoinstall auto-save

This command is used to enable automatically saving the downloaded configuration on the switch.

.

Default	Disabled
Format	`boot autoinstall auto-save`
Mode	Privileged EXEC

no boot autoinstall auto-save

This command is used to disable automatically saving the downloaded configuration on the switch.

Format	`no boot autoinstall auto-save`
Mode	Privileged EXEC

boot autoinstall start

The command is used to start Auto Install on the switch. Auto Install tries to download a config file from a TFTP server.

Format	`boot autoinstall start`
Mode	Privileged EXEC

boot autoinstall stop

The command is used to A user may terminate the Auto Install process at any time prior to the downloading of the config file. This is most optimally done when the switch is disconnected from the network, or if the requisite configuration files have not been configured on TFTP servers. Termination of the Auto Install process ends further periodic requests for a host-specific file.

Format	`boot autoinstall stop`
Mode	Privileged EXEC

boot autoinstall retry-count

This command is used to set the number of attempts to download a configuration. The valid range is from 1 to 6.

Default	3
Format	`boot autoinstall retry-count`
Mode	Privileged EXEC

no boot autoinstall retry-count

This command is used to reset the number to the default. The default number is 3.

Format	`no boot autoinstall retry-count`
Mode	Privileged EXEC

Dual Image Commands

The software supports a dual image feature that allows the switch to have two software images in the permanent storage. You can specify which image is the active image to be loaded in subsequent reboots. This feature allows reduced down-time when you upgrade or downgrade the software.

delete

This command deletes the supplied image file from the permanent storage. The image to be deleted must be a backup image. If this image is the active image, or if this image is activated, an error message displays. The optional *`<unit>`* parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. In a stack, the *`<unit>`* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format	**`delete`** *`[<unit>] {image1	image2}`*
Mode	Privileged EXEC

boot system

This command activates the specified image. It will be the active-image for subsequent reboots and will be loaded by the boot loader. The current active-image is marked as the backup-image for subsequent reboots. The optional *<unit>* parameter is valid only in Stacking, where the *unit* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format	**`boot system`** *`[<unit>] <image-file-name>`*
Mode	Privileged EXEC

show bootvar

This command displays the version information and the activation status for the current active and backup images on the supplied unit (node) of the Stack. If you do not specify a unit number, the command displays image details for all nodes on the Stack. The command also displays any text description associated with an image. This command, when used on a Standalone system, displays the switch activation status. For a standalone system, the unit parameter is not valid.

Format	**`show bootvar`** *`[<unit>]`*
Mode	Privileged EXEC

filedescr

This command associates a given text description with an image. Any existing description will be replaced. For stacking, the *[<unit>]* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format	**`filedescr`** *`[<unit>] {image1 | image2} <text-description>`*
Mode	Privileged EXEC

update bootcode

This command updates the bootcode (boot loader) on the switch. The bootcode is read from the active-image for subsequent reboots.The optional *<unit>* parameter is valid only on Stacks. Error will be returned, if this parameter is provided, on Standalone systems. For Stacking, the *<unit>* parameter identifies the node on which this command must be executed. When this parameter is not supplied, the command is executed on all nodes in a Stack.

Format	**`update bootcode`** *`[<unit>]`*
Mode	Privileged EXEC

System Information and Statistics Commands

This section describes the commands you use to view information about system features, components, and configurations.

show arp switch

This command displays the contents of the IP stack’s Address Resolution Protocol (ARP) table. The IP stack only learns ARP entries associated with the management interfaces - network or service ports. ARP entries associated with routing interfaces are not listed.

Format	`show arp switch`
Mode	Privileged EXEC

Term	Definition
IP Address	IP address of the management interface or another device on the management network.
MAC Address	Hardware MAC address of that device.
Interface	For a service port the output is *Management*. For a network port, the output is the unit/slot/port of the physical interface.

show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset. The `<unit>` is the switch identifier.

Format	**`show eventlog`** *`[<unit>]`*
Mode	Privileged EXEC

Term	Definition
File	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.
Unit	The unit for the event.

Note: Event log information is retained across a switch reset.

show hardware

This command displays inventory information for the switch.

Note: The show version command and the show hardware command display the same information. In future releases of the software, the show hardware command will not be available. For a description of the command output, see the command "show version" on page 6-8.

Format	`show hardware`
Mode	Privileged EXEC

show version

This command displays inventory information for the switch.

Note: The show version command will replace the show hardware command in future releases of the software.

Format `show version`

Mode Privileged EXEC

Term	Definition
Switch Description	Text used to identify the product name of this switch.
Machine Type	The machine model as defined by the Vital Product Data.
Machine Model	The machine model as defined by the Vital Product Data
Serial Number	The unique box serial number for this switch.
FRU Number	The field replaceable unit number.
Manufacturer	Manufacturer descriptor field.
Burned in MAC Address	Universally assigned network address.
Software Version	The release.version.revision number of the code currently running on the switch.
Additional Packages	The additional packages incorporated into this system.

show interface

This command displays a summary of statistics for a specific interface or a count of all CPU traffic based upon the argument.

Format **`show interface`** *`{<unit/slot/port> | switchport}`*

Mode Privileged EXEC

The display parameters, when the argument is `<unit/slot/port>`, are as follows:

Parameters	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is “switchport” are as follows:

Term	Definition
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Error	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.

Term	Definition
Address Entries Currently In Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently In Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

show interface ethernet

This command displays detailed statistics for a specific interface or for all CPU traffic based upon the argument.

Format	**`show interface ethernet`** *`{<unit/slot/port>	switchport}`*
Mode	Privileged EXEC

When you specify a value for *`<unit/slot/port>`*, the command displays the following information.

Term	Definition
Total Packets Received (Octets)	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Term	Definition
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries Currently in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

show mac-addr-table

This command displays the forwarding database entries. These entries are used by the transparent bridging function to determine how to forward a received frame.

Enter *`all`* or no parameter to display the entire table. Enter a MAC Address and VLAN ID to display the table entry for the requested MAC address on the specified VLAN. Enter the *`count`* parameter to view summary information about the forwarding database table. Use the *`interface <unit/slot/port>`* parameter to view MAC addresses on a specific interface. Use the *`vlan <vlan_id>`* parameter to display information about MAC addresses on a specified VLAN.

Format	**`show mac-addr-table`** *`[{<macaddr> <vlan_id> | all | count | interface <unit/slot/port> | vlan <vlan_id>}]`*
Mode	Privileged EXEC

The following information displays if you do not enter a parameter, the keyword all, or the MAC address and VLAN ID. If you enter *`vlan <vlan_id>`*, only the Mac Address, Interface, and Status fields appear.

Term	Definition
Mac Address	A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example `01:23:45:67:89:`AB. In an IVL system the MAC address will be displayed as 8 bytes.
Interface	The port through which this address was learned.
Interface Index	This object indicates the ifIndex of the interface table entry associated with this port.
Status	The status of this entry. The meanings of the values are: • *Static*—The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned. • *Learned*—The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • *Management*—The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 0/1. and is currently used when enabling VLANs for routing. • *Self*—The value of the corresponding instance is the address of one of the switch’s physical interfaces (the system’s own MAC address). • *GMRP Learned*—The value of the corresponding was learned via GMRP and applies to Multicast. • *Other*—The value of the corresponding instance does not fall into one of the other categories.

If you enter the `interface <unit/slot/port>` parameter, in addition to the MAC Address and Status fields, the following field appears:

Term	Definition
VLAN ID	The VLAN on which the MAC address was learned.

The following information displays if you enter the `count` parameter:

Term	Definition
Dynamic Address count	Number of MAC addresses in the forwarding database that were automatically learned.
Static Address (User-defined) count	Number of MAC addresses in the forwarding database that were manually entered by a user.
Total MAC Addresses in use	Number of MAC addresses currently in the forwarding database.
Total MAC Addresses available	Number of MAC addresses the forwarding database can handle.

show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Note: It is not necessarily the traffic to the CPU, but different tasks that keep the CPU busy.

Format	`show process cpu`
Mode	Privileged EXEC

The following shows example CLI display output.

```
(Switch) #show process cpu

Memory Utilization Report
status      bytes
```

```
------ ----------
  free  192980480
alloc   53409968
Task Utilization Report
Task                    Utilization
---------------------- -----------
bcmL2X.0                      0.75%
bcmCNTR.0                     0.20%
bcmLINK.0                     0.35%
DHCP snoop                    0.10%
Dynamic ARP Inspection        0.10%
dot1s_timer_task              0.10%
dhcpsPingTask                 0.20%
```

show mbuf total

This command shows the total system buffer pools status.

Format	show mbuf total
Mode	Privileged EXEC

The following shows an example of CLI display output for the command.

```
(switch) #show mbuf total

mbufSize           9284 (0x2444)
Current Time       0x1897fa
MbufsFree          150
MbufsRxUsed        0
Total Rx Norm Alloc Attempts   26212
Total Rx Mid2 Alloc Attempts   4087
Total Rx Mid1 Alloc Attempts   188943
Total Rx High Alloc Attempts   384555
Total Tx Alloc Attempts        2478536
Total Rx Norm Alloc Failures   0
Total Rx Mid2 Alloc Failures   0
Total Rx Mid1 Alloc Failures   0
Total Rx High Alloc Failures   0
Total Tx Alloc Failures        0
```

show running-config

Use this command to display or capture the current setting of different protocol packages supported on the switch. This command displays or captures commands with settings and configurations that differ from the default value. To display or capture the commands with settings and configurations that are equal to the default value, include the `[all]` option.

Note: Show running-config does not display the User Password, even if you set one different from the default.

The output is displayed in script format, which can be used to configure another switch with the same configuration. If the optional *`<scriptname>`* is provided with a file name extension of “.scr”, the output is redirected to a script file.

Note: If you issue the show running-config command from a serial connection, access to the switch through remote connections (such as Telnet) is suspended while the output is being generated and displayed.

Note: If you use a text-based configuration file, the `show running-config` command will only display configured physical interfaces, i.e. if any interface only contains the default configuration, that interface will be skipped from the `show running-config` command output. This is true for any configuration mode that contains nothing but default configuration. That is, the command to enter a particular config mode, followed immediately by its ‘exit’ command, are both omitted from the `show running-config` command output (and hence from the startup-config file when the system configuration is saved.)

If option <`changed`> is used, this command displays/capture commands with settings/ configurations that differ from the default value.

- If all the flags in a particular group are enabled, then the command displays **`trapflags`** *`<group name>`* **`all`**.
- If some, but not all, of the flags in that group are enabled, the command displays **`trapflags`** *`<groupname> <flag-name>.`*

Format	**`show running-config`** *`[all	<scriptname>	changed]`*
Mode	Privileged EXEC

show running-config interface

This command shows the current configuration on a particular interface. The interface could be a physical port or a virtual port—like a LAG or VLAN. The output captures how the configuration differs from the factory default value.

Format	**show running-config interface** *{<unit/slot/port>} | VLAN <id> | LAG <id>}*
Mode	Interface Config

show sysinfo

This command displays switch information.

Format	**`show sysinfo`**
Mode	Privileged EXEC

Term	Definition
Switch Description	Text used to identify this switch.
System Name	Name used to identify the switch.The factory default is blank. To configure the system name, see “snmp-server” on page 7-47.
System Location	Text used to identify the location of the switch. The factory default is blank. To configure the system location, see “snmp-server” on page 7-47.
System Contact	Text used to identify a contact person for this switch. The factory default is blank. To configure the system location, see “snmp-server” on page 7-47.
System Object ID	The base object ID for the switch’s enterprise MIB.
System Up Time	The time in days, hours and minutes since the last switch reboot.
MIBs Supported	A list of MIBs supported by this agent.

show tech-support

Use the **`show tech-support`** command to display system and configuration information when you contact technical support. The output of the **`show tech-support`** command combines the output of the following commands:

- show version
- show sysinfo

- show port all
- show isdp neighbors
- show logging
- show event log
- show logging buffered
- show trap log

Format	`show tech-support`
Mode	Privileged EXEC

terminal length

Use this command to set the number of lines of output to be displayed on the screen, i.e. pagination, for the **`show running-config`** and **`show running-config all`** commands. The terminal length size is either zero or a number in the range of 5 to 48. After the user-configured number of lines is displayed in one page, the system prompts the user "`--More-- or (q)uit.`" Press `q` or `Q` to quit, or press any key to display the next set of <*5-48*> lines. The command **`terminal length 0`** disables pagination and, as a result, the output of the **`show running-config`** command is displayed immediately.

Default	24 lines per page
Format	**`terminal length <`**`0`**`|`***`5-48`***`>`**
Mode	Privileged EXEC

no terminal length

Use this command to set the terminal length to the default value.

Format	`no terminal length`
Mode	Privileged EXEC

show terminal length

Use this command to display the value of the user-configured terminal length size.

Format	`show terminal length`
Mode	Privileged EXEC

Logging Commands

This section describes the commands you use to configure system logging, and to view logs and the logging settings.

logging buffered

This command enables logging to an in-memory log that keeps up to 128 logs.

Default	disabled; critical when enabled
Format	`logging buffered`
Mode	Global Config

no logging buffered

This command disables logging to in-memory log.

Format	`no logging buffered`
Mode	Global Config

logging buffered wrap

This command enables wrapping of in-memory logging when the log file reaches full capacity. Otherwise when the log file reaches full capacity, logging stops.

Default	enabled
Format	`logging buffered wrap`
Mode	Privileged EXEC

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when the log file capacity is full.

Format	`no logging buffered wrap`
Mode	Privileged EXEC

logging cli-command

This command enables the CLI command logging feature, which enables the 7000 series software to log all CLI commands issued on the system.

Default	enabled
Format	`logging cli-command`
Mode	Global Config

no logging cli-command

This command disables the CLI command Logging feature.

Format	`no logging cli-command`
Mode	Global Config

logging console

This command enables logging to the console. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	disabled; critical when enabled
Format	**logging console** *[severitylevel]*
Mode	Global Config

no logging console

This command disables logging to the console.

Format	`no logging console`
Mode	Global Config

logging host

This command enables logging to a host. You can configure up to eight hosts. The *<ipaddr|hostname>* is the IP address of the logging host. The *<addresstype>* indicates the type of address ipv4 or ipv6 or dns being passed. The *<port>* value is a port number from 1 to 65535. You can specify the *<severitylevel>* value as either an integer from 0 to 7 or symbolically through one of the following keywords: **emergency** (0), **alert** (1), **critical** (2), **error** (3), **warning** (4), **notice** (5), **info** (6), or **debug** (7).

Default	• port—514 • level—critical (2)
Format	**logging host** *<ipaddr|hostname> <addresstype> [<port>][<severitylevel>]*
Mode	Global Config

logging host remove

This command disables logging to host. See "show logging hosts" on page 6-22 for a list of host indexes.

Format	**logging host remove** *<hostindex>*
Mode	Global Config

logging syslog

This command enables syslog logging. The *<portid>* parameter is an integer with a range of 1-65535.

Default	disabled
Format	**logging syslog** *[port <portid>]*
Mode	Global Config

no logging syslog

This command disables syslog logging.

Format `no logging syslog`

Mode Global Config

show logging

This command displays logging configuration information.

Format `show logging`

Mode Privileged EXEC

Term	Definition
Logging Client Local Port	Port on the collector/relay to which syslog messages are sent.
CLI Command Logging	Shows whether CLI Command logging is enabled.
Console Logging	Shows whether console logging is enabled.
Console Logging Severity Filter	The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
Buffered Logging	Shows whether buffered logging is enabled.
Syslog Logging	Shows whether syslog logging is enabled.
Log Messages Received	Number of messages received by the log process. This includes messages that are dropped or ignored.
Log Messages Dropped	Number of messages that could not be processed due to error or lack of resources.
Log Messages Relayed	Number of messages sent to the collector/relay.

show logging buffered

This command displays buffered logging (system startup and system operation logs).

Format `show logging buffered`

Mode Privileged EXEC

Term	Definition
Buffered (In-Memory) Logging	Shows whether the In-Memory log is enabled or disabled.
Buffered Logging Wrapping Behavior	The behavior of the In Memory log when faced with a log full situation.
Buffered Log Count	The count of valid entries in the buffered log.

show logging hosts

This command displays all configured logging hosts. The `<unit>` is the switch identifier and has a range of 1-8.

Format	**`show logging hosts`** *`<unit>`*
Mode	Privileged EXEC

Term	Definition
Host Index	(Used for deleting hosts.)
IP Address / Hostname	IP address or hostname of the logging host.
Severity Level	The minimum severity to log to the specified address. The possible values are emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), info (6), or debug (7).
Port	The server port number, which is the port on the local host from which syslog messages are sent.
Host Status	The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

show logging traplogs

This command displays SNMP trap events and statistics.

Format	`show logging traplogs`
Mode	Privileged EXEC

Term	Definition
Number of Traps Since Last Reset	The number of traps since the last boot.
Trap Log Capacity	The number of traps the system can retain.
Number of Traps Since Log Last Viewed	The number of new traps since the command was last executed.
Log	The log number.
System Time Up	How long the system had been running at the time the trap was sent.
Trap	The text of the trap message.

logging persistent

Use this command to configure the Persistent logging for the switch. The severity level of logging messages is specified at severity level. Possible values for severity level are *`(emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7)`*.

Default	Disable
Format	**`logging persistent`** *`<severity level>`*
Mode	Global Config

no logging persistent

Use this command to disable the persistent logging in the switch.

Format	`no logging persistent`
Mode	Global Config

System Utility and Clear Commands

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

traceroute

Use the `traceroute` command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Default	• count: 3 probes • interval: 3 seconds • size: 0 bytes • port: 33434 • maxTtl: 30 hops • maxFail: 5 probes • initTtl: 1 hop •
Format	**traceroute** *<ipaddr|hostname>* [**initTtl** *<initTtl>*] [**maxTtl** *<maxTtl>*] [**maxFail** *<maxFail>*] [**interval** *<interval>*] [**count** *<count>*] [**port** *<port>*] [**size** *<size>*]
Mode	Privileged EXEC

Using the options described below, you can specify the initial and maximum time-to-live (TTL) in probe packets, the maximum number of failures before termination, the number of probes sent for each TTL, and the size of each probe.

Parameter	Description
ipaddr|hostname	The *ipaddr* value should be a valid IP address. The *hostname* value should be a valid hostname.
initTtl	Use `initTtl` to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use `maxTtle` to specify the maximum TTL. Range is 1 to 255.
maxFail	Use `maxFail` to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
interval	Use `interval` to specify the time between probes, in seconds. Range is 1 to 60 seconds.
count	Use the optional `count` parameter to specify the number of probes to send for each TTL value. Range is 1 to 10 probes.
port	Use the optional `port` parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.
size	Use the optional `size` parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

Example: The following are examples of the CLI command.

traceroute Success:

```
(Switch) # traceroute 10.240.10.115 initTtl 1 maxTtl 4 maxFail 0 interval 1 count
3 port 33434 size 43
 Traceroute to 10.240.10.115 ,4 hops max 43 byte packets:
1 10.240.4.1   708 msec     41 msec     11 msec
2 10.240.10.115   0 msec     0 msec     0 msec

Hop Count = 1 Last TTL = 2 Test attempt = 6 Test Success = 6
```

traceroute Failure:

```
(Switch) # traceroute 10.40.1.1 initTtl 1 maxFail 0 interval 1 count 3
port 33434 size 43
Traceroute to 10.40.1.1 ,30 hops max 43 byte packets:
1 10.240.4.1   19 msec     18 msec     9 msec
2 10.240.1.252   0 msec     0 msec     1 msec
3 172.31.0.9   277 msec     276 msec     277 msec
4 10.254.1.1   289 msec     327 msec     282 msec
5 10.254.21.2   287 msec     293 msec     296 msec
6 192.168.76.2   290 msec     291 msec     289 msec
7 0.0.0.0   0 msec *
Hop Count = 6 Last TTL = 7 Test attempt = 19 Test Success = 18
```

traceroute ipv6

Use the **`traceroute`** command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The *`<ipv6-address|hostname>`* parameter must be a valid IPv6 address or hostname. The optional *`<port>`* parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. The range for *`<port>`* is zero (0) to 65535. The default value is 33434.

Default	port: 33434
Format	**`traceroute ipv6`** *`<ipv6-address|hostname>`* `[`**`port`** *`<port>`*`]`
Mode	Privileged EXEC

clear config

This command resets the configuration to the factory defaults without powering off the switch. When you issue this command, a prompt appears to confirm that the reset should proceed. When you enter **`y`**, you automatically reset the current configuration on the switch to the default values. It does not reset the switch.

Format	`clear config`
Mode	Privileged EXEC

clear mac-addr-table

This command clears the dynamically learned MAC addresses of the switch.

Format	**`clear mac-addr-table`**
Mode	Privileged EXEC

clear logging buffered

This command clears the messages maintained in the system log.

Format	**`clear logging buffered`**
Mode	Privileged EXEC

clear counters

This command clears the statistics for a specified *`<unit/slot/port>,`* for all the ports, or for the entire switch based upon the argument.

Format	**`clear counters`** *`{<unit/slot/port>	all}`*
Mode	Privileged EXEC

clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and attempts to delete these entries from the Multicast Forwarding Database.

Format	`clear igmpsnooping`
Mode	Privileged EXEC

clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format	`clear pass`
Mode	Privileged EXEC

clear port-channel

This command clears all port-channels (LAGs).

Format	`clear port-channel`
Mode	Privileged EXEC

clear traplog

This command clears the trap log.

Format	`clear traplog`
Mode	Privileged EXEC

clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format	`clear vlan`
Mode	Privileged EXEC

enable password

This command prompts you to change the Privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case sensitive. The option [encrypted] allows the administrator to transfer the enable password between devices without having to know the password. In this case, the <password> parameter must be exactly 128 hexadecimal characters.

Format	`enable password <password> [encrypted]`
Mode	Privileged EXEC

logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format	`logout`
Modes	• Privileged EXEC • User EXEC

ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI and Web interfaces.

Default	• The default count is 1. • The default interval is 3 seconds. • The default size is 0 bytes.
Format	**ping** *<ipaddress|hostname>* **[count** *<count>***] [interval** *<interval>***] [size** *<size>***]**
Modes	• Privileged EXEC • User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Description
count	Use the **`count`** parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the *`<ip-address>`* field. The range for *`<count>`* is 1 to 15 requests.
interval	Use the **`interval`** parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the **`size`** parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.

The following are examples of the CLI command.

ping success:

```
(Switch) #ping 10.254.2.160 count 3 interval 1 size 255
Pinging 10.254.2.160 with 255 bytes of data:

Received response for icmp_seq = 0. time= 275268 usec
Received response for icmp_seq = 1. time= 274009 usec
Received response for icmp_seq = 2. time= 279459 usec

----10.254.2.160 PING statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 274/279/276
```

ping failure:

In Case of Unreachable Destination:

```
(Switch) # ping 192.168.254.222 count 3 interval 1 size 255
Pinging 192.168.254.222 with 255 bytes of data:
Received Response: Unreachable Destination
Received Response :Unreachable Destination
Received Response :Unreachable Destination
----192.168.254.222  PING statistics----
3 packets transmitted,3 packets received, 0% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

In Case Of Request TimedOut:

```
(Switch) # ping 1.1.1.1 count 1 interval 3
Pinging 1.1.1.1 with 0 bytes of data:

----1.1.1.1 PING statistics----
```

```
1 packets transmitted,0 packets received, 100% packet loss
round-trip (msec) min/avg/max = 0/0/0
```

quit

This command closes the current telnet connection or resets the current serial connection. The system asks you whether to save configuration changes before quitting.

Format	`quit`
Modes	• Privileged EXEC • User EXEC

reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

Format	**`reload`**
Mode	Privileged EXEC

save

This command makes the current configuration changes permanent by writing the configuration changes to system NVRAM.

Format	**save**
Mode	Privileged EXEC

copy

The **copy** command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (*image1* and *image2*) on the file system. Upload and download files from a server by using TFTP or Xmodem. SFTP and SCP are available as additional transfer methods if the software package supports secure management.

Format	**copy** `<source> <destination>`
Mode	Privileged EXEC

Replace the `<source>` and `<destination>` parameters with the options in table below. For the `<url>` source or destination, use one of the following values:

```
{xmodem | tftp://<ipaddr|hostname>|<ip6address|hostname>/<filepath>/<filename>
[noval]
| sftp|scp://<username>@<ipaddr>|<ipv6address>|<filepath>|<filename>}
```

For TFTP, SFTP and SCP, the `<ipaddr|hostname>` parameter is the IP address or host name of the server, `<filepath>` is the path to the file, and `<filename>` is the name of the file you want to upload or download. For SFTP and SCP, the <username> parameter is the username for logging into the remote server via SSH.

Note: `<ip6address>` is also a valid parameter for routing packages that support IPv6.

For platforms that support a USB device, the `copy` command can be used to transfer files from and to the USB device. The syntax for the USB file is: `usb://<filename>`. The USB device can be either a source or destination in the copy command. It cannot be used as both source and destination in a given `copy` command.

Warning: Remember to upload the existing Switch CLI.cfg file off the switch prior to loading a new release image in order to make a backup.

Parameters for the `copy` command are listed in the following table:

Source	Destination	Description
nvram:backup-config	nvram:startup-config	Copies the backup configuration to the startup configuration.
nvram:clibanner	<url>	Copies the CLI banner to a server.

Source	Destination	Description
nvram:errorlog	<url>	Copies the error log file to a server.
nvram:Switch CLI.cfg	<url>	Uploads the binary config file to a server.
nvram:log	<url>	Copies the log file to a server.
nvram:script <scriptname>	<url>	Copies a specified configuration script file to a server.
nvram:startup-config	nvram:backup-config	Copies the startup configuration to the backup configuration.
nvram:startup-config	<url>	Copies the startup configuration to a server.
nvram:traplog	<url>	Copies the trap log file to a server.
system:running-config	nvram:startup-config	Saves the running configuration to nvram.
<url>	nvram:clibanner	Downloads the CLI banner to the system.
<url>	nvram:Switch CLI.cfg	Downloads the binary config file to the system.
<url>	nvram:script <destfilename>	Downloads a configuration script file to the system. During the download of a configuration script, the copy command validates the script. In case of any error, the command lists all the lines at the end of the validation process and prompts you to confirm before copying the script file.
<url>	nvram:script <destfilename> noval	When you use this option, the copy command will not validate the downloaded script file. An example of the CLI command follows: `(NETGEAR Switch) #copy tftp://1.1.1.1/ file.scr nvram:script file.scr`
<url>	nvram:sshkey-dsa	Downloads an SSH key file. For more information, see "Secure Shell (SSH) Commands" on page 7-16.
<url>	nvram:sshkey-rsa1	Downloads an SSH key file.
<url>	nvram:sshkey-rsa2	Downloads an SSH key file.
<url>	nvram:sslpem-dhweak	Downloads an HTTP secure-server certificate.
<url>	nvram:sslpem-dhstrong	Downloads an HTTP secure-server certificate.
<url>	nvram:sslpem-root	Downloads an HTTP secure-server certificate. For more information, see "Hypertext Transfer Protocol (HTTP) Commands" on page 7-20.
<url>	nvram:sslpem-server	Downloads an HTTP secure-server certificate.
<url>	nvram:startup-config	Downloads the startup configuration file to the system.
<url>	nvram:system-image	Downloads a code image to the system.
<url>	nvram:license-key	Download the license date to the system.
<url>	ias-users	Downloads IAS users file by sftp, scp or tftp

Source	Destination	Description
<url>	{image1 | image2}	Download an image from the remote server to either image. In a stacking environment, the downloaded image is distributed to the stack nodes.
{image1 | image2}	<url>	Upload either image to the remote server.
image1	image2	Copy **`image1`** to **`image2`**.
image2	image1	Copy **`image2`** to **`image1`**.
{image1 | image2}	unit://<unit>/{image1 | image2}	Copy an image from the management node to a given node in a Stack. Use the unit parameter to specify the node to which the image should be copied.
{image1 | image2}	unit://*/{image1 | image2}	Copy an image from the management node to all of the nodes in a Stack.

write memory

Use this command to save running configuration changes to NVRAM so that the changes you make will persist across a reboot. This command is the same as `copy system:running config nvram:startup-config`.

Format `write memory`

Mode Privileged EXEC

Simple Network Time Protocol (SNTP) Commands

This section describes the commands you use to automatically configure the system time and date by using SNTP.

sntp broadcast client poll-interval

This command sets the poll interval for SNTP broadcast clients in seconds as a power of two where *`<poll-interval>`* can be a value from 6 to 10.

Default 6

Format **`sntp broadcast client poll-interval`** *`<poll-interval>`*

Mode Global Config

no sntp broadcast client poll-interval

This command resets the poll interval for SNTP broadcast client back to the default value.

Format	`no sntp broadcast client poll-interval`
Mode	Global Config

sntp client mode

This command enables Simple Network Time Protocol (SNTP) client mode and may set the mode to either broadcast or unicast.

Default	disabled
Format	**`sntp client mode`** *`[broadcast	unicast]`*
Mode	Global Config

no sntp client mode

This command disables Simple Network Time Protocol (SNTP) client mode.

Format	`no sntp client mode`
Mode	Global Config

sntp client port

This command sets the SNTP client port id to a value from 1-65535.

Default	123
Format	**`sntp client port`** *`<portid>`*
Mode	Global Config

no sntp client port

This command resets the SNTP client port back to its default value.

Format	`no sntp client port`
Mode	Global Config

sntp unicast client poll-interval

This command sets the poll interval for SNTP unicast clients in seconds as a power of two where `<poll-interval>` can be a value from 6 to 10.

Default	6
Format	**`sntp unicast client poll-interval`** *`<poll-interval>`*
Mode	Global Config

no sntp unicast client poll-interval

This command resets the poll interval for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-interval`
Mode	Global Config

sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds to a value from 1-30.

Default	5
Format	**`sntp unicast client poll-timeout`** *`<poll-timeout>`*
Mode	Global Config

no sntp unicast client poll-timeout

This command will reset the poll timeout for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-timeout`
Mode	Global Config

sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients to a value from 0 to 10.

Default	1

Format	**`sntp unicast client poll-retry`** *`<poll-retry>`*
Mode	Global Config

no sntp unicast client poll-retry

This command will reset the poll retry for SNTP unicast clients to its default value.

Format	`no sntp unicast client poll-retry`
Mode	Global Config

sntp server

This command configures an SNTP server (a maximum of three). The optional priority can be a value of 1-3, the version a value of 1-4, and the port id a value of 1-65535.

Format	**`sntp server`** *`<ipaddress|ipv6address| hostname> [<priority> [<version> [<portid>]]]`*
Mode	Global Config

no sntp server

This command deletes an server from the configured SNTP servers.

Format	**`no sntp server remove`** *`<ipaddress|ipv6address| hostname>`*
Mode	Global Config

clock timezone

When using SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on Coordinated Universal Time (UTC) which is the same as Greenwich Mean Time (GMT). This may not be the time zone in which the switch is located. Use the **clock timezone** command to configure a time zone specifying the number of hours and optionally the number of minutes difference from UTC. To set the switch clock to UTC, use the **no** form of the command.

Format	**`clock timezone`** *zone-name +/-hours-offset [+/-minutes-offset]*

Mode	Global Config
Default	**`no clock timezone`**

Zone name: A name to associate with the time zone

Hours-offset: Number of hours difference with UTC

Minutes-offset: Number of minutes difference with UTC

no clock timezone

This command sets the switch to UTC time.

Format	**`no clock timezone`**
Mode	Global Config

show sntp

This command is used to display SNTP settings and status.

Format	`show sntp`
Mode	Privileged EXEC

Term	Definition
Last Update Time	Time of last clock update.
Last Unicast Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
Broadcast Count	Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
Multicast Count	Current number of unsolicited multicast messages that have been received and processed by the SNTP client since last reboot.

show sntp client

This command is used to display SNTP client settings.

Format `show sntp client`

Mode Privileged EXEC

Term	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port.
Client Mode	Configured SNTP Client Mode.

show sntp server

This command is used to display SNTP server settings and configured servers.

Format `show sntp server`

Mode Privileged EXEC

Term	Definition
Server Host Address	IP address or hostname of configured SNTP Server.
Server Type	Address Type of Server.
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference ID	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.

For each configured server:

Term	Definition
Host Address	IP address or hostname of configured SNTP Server.
Address Type	Address Type of configured SNTP server.
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number.
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

show clock

This command is used to display the time information.

Format	`show clock [detail]`
Mode	Privileged EXEC

Term	Definition
Time	The time provided by the time source.
Time Source	The time source type.
If option *detail* is specified, these terms are displayed	
Time Zone	The time zone configured.
Summer Time	Indicate if the summer time is enabled.

DHCP Server Commands

This section describes the commands you to configure the DHCP server settings for the switch. DHCP uses UDP as its transport protocol and supports a number of features that facilitate in administration address allocations.

ip dhcp pool

This command configures a DHCP address pool name on a DHCP server and enters DHCP pool configuration mode.

Default	none
Format	**`ip dhcp pool`** `<`*`name`*`>`
Mode	Global Config

no ip dhcp pool

This command removes the DHCP address pool. The name should be previously configured pool name.

Format	**`no ip dhcp pool`** `<`*`name`*`>`
Mode	Global Config

client-identifier

This command specifies the unique identifier for a DHCP client. Unique-identifier is a valid notation in hexadecimal format. In some systems, such as Microsoft DHCP clients, the client identifier is required instead of hardware addresses. The unique-identifier is a concatenation of the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address c819.2488.f177 is 01c8.1924.88f1.77 where 01 represents the Ethernet media type. For more information, refer to the “Address Resolution Protocol Parameters” section of RFC 1700, Assigned Numbers for a list of media type codes.

Default	none
Format	**`client-identifier`** `<`*`uniqueidentifier`*`>`
Mode	DHCP Pool Config

no client-identifier

This command deletes the client identifier.

Format	`no client-identifier`
Mode	DHCP Pool Config

client-name

This command specifies the name for a DHCP client. Name is a string consisting of standard ASCII characters.

Default	none
Format	**`client-name`** *`<name>`*
Mode	DHCP Pool Config

no client-name

This command removes the client name.

Format	`no client-name`
Mode	DHCP Pool Config

default-router

This command specifies the default router list for a DHCP client. {*`address1, address2`*… *`address8`*} are valid IP addresses, each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	**`default-router`** *`<address1> [<address2>....<address8>]`*
Mode	DHCP Pool Config

no default-router

This command removes the default router list.

Format	`no default-router`
Mode	DHCP Pool Config

dns-server

This command specifies the IP servers available to a DHCP client. Address parameters are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Default	none
Format	**`dns-server`** *`<address1> [<address2>....<address8>]`*
Mode	DHCP Pool Config

no dns-server

This command removes the DNS Server list.

Format	`no dns-server`
Mode	DHCP Pool Config

hardware-address

This command specifies the hardware address of a DHCP client. Hardware-address is the MAC address of the hardware platform of the client consisting of 6 bytes in dotted hexadecimal format. Type indicates the protocol of the hardware platform. It is 1 for 10 MB Ethernet and 6 for IEEE 802.

Default	ethernet
Format	**`hardware-address`** *`<hardwareaddress> <type>`*
Mode	DHCP Pool Config

no hardware-address

This command removes the hardware address of the DHCP client.

Format	`no hardware-address`
Mode	DHCP Pool Config

host

This command specifies the IP address and network mask for a manual binding to a DHCP client. Address and Mask are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. The prefix-length is an integer from 0 to 32.

Default	none
Format	**host** *<address> [{<mask> | <prefix-length>}]*
Mode	DHCP Pool Config

no host

This command removes the IP address of the DHCP client.

Format	`no host`
Mode	DHCP Pool Config

lease

This command configures the duration of the lease for an IP address that is assigned from a DHCP server to a DHCP client. The overall lease time should be between 1-86400 minutes. If you specify *infinite*, the lease is set for 60 days. You can also specify a lease duration. *Days* is an integer from 0 to 59. *Hours* is an integer from 0 to 23. *Minutes* is an integer from 0 to 59.

Default	1 (day)
Format	**lease** *[{<days> [<hours>] [<minutes>] | infinite}]*
Mode	DHCP Pool Config

no lease

This command restores the default value of the lease time for DHCP Server.

Format	`no lease`
Mode	DHCP Pool Config

network (DHCP Pool Config)

Use this command to configure the subnet number and mask for a DHCP address pool on the server. Network-number is a valid IP address, made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid. Mask is the IP subnet mask for the specified address pool. The prefix-length is an integer from 0 to 32.

Default	none
Format	**`network`** *`<networknumber> [{<mask>	<prefixlength>}]`*
Mode	DHCP Pool Config

no network

This command removes the subnet number and mask.

Format	`no network`
Mode	DHCP Pool Config

bootfile

The command specifies the name of the default boot image for a DHCP client. The *`<filename>`* specifies the boot image file.

Format	**`bootfile`** *`<filename>`*
Mode	DHCP Pool Config

no bootfile

This command deletes the boot image name.

Format	`no bootfile`
Mode	DHCP Pool Config

domain-name

This command specifies the domain name for a DHCP client. The *`<domain>`* specifies the domain name string of the client.

Default	none
Format	**`domain-name`** *`<domain>`*
Mode	DHCP Pool Config

no domain-name

This command removes the domain name.

Format	`no domain-name`
Mode	DHCP Pool Config

netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to DHCP clients.

One IP address is required, although one can specify up to eight addresses in one command line. Servers are listed in order of preference (address1 is the most preferred server, address2 is the next most preferred server, and so on).

Default	none
Format	**`netbios-name-server`** *`<address> [<address2>...<address8>]`*
Mode	DHCP Pool Config

no netbios-name-server

This command removes the NetBIOS name server list.

Format	`no netbios-name-server`
Mode	DHCP Pool Config

netbios-node-type

The command configures the NetBIOS node type for Microsoft Dynamic Host Configuration Protocol (DHCP) clients.type Specifies the NetBIOS node type. Valid types are:

- b-node—Broadcast
- p-node—Peer-to-peer
- m-node—Mixed
- h-node—Hybrid (recommended)

Default	none
Format	**`netbios-node-type`** *`<type>`*
Mode	DHCP Pool Config

no netbios-node-type

This command removes the NetBIOS node Type.

Format	`no netbios-node-type`
Mode	DHCP Pool Config

next-server

This command configures the next server in the boot process of a DHCP client.The *`<address>`* parameter is the IP address of the next server in the boot process, which is typically a TFTP server.

Default	inbound interface helper addresses
Format	**`next-server`** *`<address>`*
Mode	DHCP Pool Config

no next-server

This command removes the boot server list.

Format	`no next-server`
Mode	DHCP Pool Config

option

The **`option`** command configures DHCP Server options. The *`<code>`* parameter specifies the DHCP option code and ranges from 1-254. The *`<ascii string>`* parameter specifies an NVT ASCII character string. ASCII character strings that contain white space must be delimited by quotation marks. The *`hex <string>`* parameter specifies hexadecimal data. In hexadecimal, character strings are two hexadecimal digits. You can separate each byte by a period (for example, `a3.4f.22.0c`), colon (for example, `a3:4f:22:0c`), or white space (for example, `a3 4f 22 0c`).

Default	none
Format	**`option`** *`<code> {ascii string | hex <string1> [<string2>...<string8>] | ip <address1> [<address2>...<address8>]}`*
Mode	DHCP Pool Config

no option

This command removes the DHCP Server options. The *`<code>`* parameter specifies the DHCP option code.

Format	**`no option`** *`<code>`*
Mode	DHCP Pool Config

ip dhcp excluded-address

This command specifies the IP addresses that a DHCP server should not assign to DHCP clients. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address `0.0.0.0` is invalid.

Default	none

Format	**`ip dhcp excluded-address`** *`<lowaddress> [highaddress]`*
Mode	Global Config

no ip dhcp excluded-address

This command removes the excluded IP addresses for a DHCP client. Low-address and high-address are valid IP addresses; each made up of four decimal bytes ranging from 0 to 255. IP address 0.0.0.0 is invalid.

Format	**`no ip dhcp excluded-address`** *`<lowaddress> [highaddress]`*
Mode	Global Config

ip dhcp ping packets

Use this command to specify the number, in a range from 2-10, of packets a DHCP server sends to a pool address as part of a ping operation. By default the number of packets sent to a pool address is 2, which is the smallest allowed number when sending packets. Setting the number of packets to 0 disables this command.

Default	2
Format	**`ip dhcp ping packets`** *`<0,2-10>`*
Mode	Global Config

no ip dhcp ping packets

This command prevents the server from pinging pool addresses and sets the number of packets to 0.

Default	0
Format	`no ip dhcp ping packets`
Mode	Global Config

service dhcp

This command enables the DHCP server.

Default	disabled
Format	`service dhcp`
Mode	Global Config

no service dhcp

This command disables the DHCP server.

Format	`no service dhcp`
Mode	Global Config

ip dhcp bootp automatic

This command enables the allocation of the addresses to the bootp client. The addresses are from the automatic address pool.

Default	disabled
Format	`ip dhcp bootp automatic`
Mode	Global Config

no ip dhcp bootp automatic

This command disables the allocation of the addresses to the bootp client. The address are from the automatic address pool.

Format	`no ip dhcp bootp automatic`
Mode	Global Config

ip dhcp conflict logging

This command enables conflict logging on DHCP server.

Default	enabled
Format	`ip dhcp conflict logging`
Mode	Global Config

no ip dhcp conflict logging

This command disables conflict logging on DHCP server.

Format	`no ip dhcp conflict logging`
Mode	Global Config

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database. If "*" is specified, the bindings corresponding to all the addresses are deleted. `<address>` is a valid IP address made up of four decimal bytes ranging from 0 to 255. IP address `0.0.0.0` is invalid.

Format	**`clear ip dhcp binding`** *`{<address>	*}`*
Mode	Privileged EXEC

clear ip dhcp server statistics

This command clears DHCP server statistics counters.

Format	`clear ip dhcp server statistics`
Mode	Privileged EXEC

clear ip dhcp conflict

The command is used to clear an address conflict from the DHCP Server database. The server detects conflicts using a ping. DHCP server clears all conflicts If the asterisk (*) character is used as the address parameter.

Default	none
Format	**`clear ip dhcp conflict`** *`{<address> | *}`*
Mode	Privileged EXEC

show ip dhcp binding

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	**`show ip dhcp binding`** *`[<address>]`*
Modes	• Privileged EXEC • User EXEC

Term	Definition
IP address	The IP address of the client.
Hardware Address	The MAC Address or the client identifier.
Lease expiration	The lease expiration time of the IP address assigned to the client.
Type	The manner in which IP address was assigned to the client.

show ip dhcp global configuration

This command displays address bindings for the specific IP address on the DHCP server. If no IP address is specified, the bindings corresponding to all the addresses are displayed.

Format	`show ip dhcp global configuration`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Service DHCP	The field to display the status of dhcp protocol.

Term	Definition
Number of Ping Packets	The maximum number of Ping Packets that will be sent to verify that an ip address id not already assigned.
Conflict Logging	Shows whether conflict logging is enabled or disabled.
BootP Automatic	Shows whether BootP for dynamic pools is enabled or disabled.

show ip dhcp pool configuration

This command displays pool configuration. If **`all`** is specified, configuration for all the pools is displayed.

Format	**`show ip dhcp pool configuration`** *`{<name>	all}`*
Modes	• Privileged EXEC • User EXEC

Field	Definition
Pool Name	The name of the configured pool.
Pool Type	The pool type.
Lease Time	The lease expiration time of the IP address assigned to the client.
DNS Servers	The list of DNS servers available to the DHCP client .
Default Routers	The list of the default routers available to the DHCP client

The following additional field is displayed for Dynamic pool type:

Field	Definition
Network	The network number and the mask for the DHCP address pool.

The following additional fields are displayed for Manual pool type:

Field	Definition
Client Name	The name of a DHCP client.
Client Identifier	The unique identifier of a DHCP client.
Hardware Address	The hardware address of a DHCP client.
Hardware Address Type	The protocol of the hardware platform.
Host	The IP address and the mask for a manual binding to a DHCP client.

show ip dhcp server statistics

This command displays DHCP server statistics.

Format	`show ip dhcp server statistics`
Modes	• Privileged EXEC • User EXEC

Field	Definition
Automatic Bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired Bindings	The number of expired leases.
Malformed Bindings	The number of truncated or corrupted messages that were received by the DHCP server.

Message Received:

Message	Definition
DHCP DISCOVER	The number of DHCPDISCOVER messages the server has received.
DHCP REQUEST	The number of DHCPREQUEST messages the server has received.
DHCP DECLINE	The number of DHCPDECLINE messages the server has received.
DHCP RELEASE	The number of DHCPRELEASE messages the server has received.
DHCP INFORM	The number of DHCPINFORM messages the server has received.

Message Sent:

Message	Definition
DHCP OFFER	The number of DHCPOFFER messages the server sent.
DHCP ACK	The number of DHCPACK messages the server sent.
DHCP NACK	The number of DHCPNACK messages the server sent.

show ip dhcp conflict

This command displays address conflicts logged by the DHCP Server. If no IP address is specified, all the conflicting addresses are displayed.

Format	**`show ip dhcp conflict`** *`[<ip-address>]`*
Modes	• Privileged EXEC • User EXEC

Term	Definition
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP Server.
Detection time	The time when the conflict was found.

DNS Client Commands

These commands are used in the Domain Name System (DNS), an Internet directory service. DNS is how domain names are translated into IP addresses. When enabled, the DNS client provides a hostname lookup service to other components.

ip domain lookup

Use this command to enable the DNS client.

Default	enabled
Format	`ip domain lookup`
Mode	Global Config

no ip domain lookup

Use this command to disable the DNS client.

Format	`no ip domain lookup`
Mode	Global Config

ip domain name

Use this command to define a default domain name that the software uses to complete unqualified host names (names with a domain name). By default, no default domain name is configured in the system. <*name*> may not be longer than 255 characters and should not include an initial period. This <*name*> should be used only when the default domain name list, configured using the **ip domain list** command, is empty.

Default	none
Format	**ip domain name** <*name*>
Mode	Global Config

Example: The CLI command **ip domain name yahoo.com** will configure yahoo.com as a default domain name. For an unqualified hostname xxx, a DNS query is made to find the IP address corresponding to xxx.yahoo.com.

no ip domain name

Use this command to remove the default domain name configured using the **ip domain name** command.

Format	no ip domain name
Mode	Global Config

ip domain list

Use this command to define a list of default domain names to complete unqualified names. By default, the list is empty. Each name must be no more than 256 characters, and should not include an initial period. The default domain name, configured using the **ip domain name** command, is used only when the default domain name list is empty. A maximum of 32 names can be entered in to this list.

Default	none
Format	**ip domain list** <*name*>
Mode	Global Config

no ip domain list

Use this command to delete a name from a list.

Format	**no ip domain list** *<name>*
Mode	Global Config

ip name server

Use this command to configure the available name servers. Up to eight servers can be defined in one command or by using multiple commands. The parameter `<server-address>` is a valid IPv4 or IPv6 address of the server. The preference of the servers is determined by the order they were entered.

Format	**ip name-server <***server-address1***> [***server-address2...server-address8***]**
Mode	Global Config

no ip name server

Use this command to remove a name server.

Format	**no ip name-server [***server-address1...server-address8***]**
Mode	Global Config

ip host

Use this command to define static host name-to-address mapping in the host cache. <*name*> is host name. <i*p address*> is the IP address of the host.

Default	none
Format	**ip host <***name***> <***ipaddress***>**
Mode	Global Config

no ip host

Use this command to remove the name-to-address mapping.

Format	**`no ip host <`***`name`***`>`**
Mode	Global Config

ipv6 host

Use this command to define static host name-to-IPv6 address mapping in the host cache. <*`name`*> is host name. <v6 *`address`*> is the IPv6 address of the host.

Default	none
Format	**`ipv6 host <`***`name`***`> <`***`v6 address`***`>`**
Mode	Global Config

no ipv6 host

Use this command to remove the static host name-to-IPv6 address mapping in the host cache.

Format	**`no ipv6 host <`***`name`***`>`**
Mode	Global Config

ip domain retry

Use this command to specify the number of times to retry sending Domain Name System (DNS) queries. The parameter <*`number`*> indicates the number of times to retry sending a DNS query to the DNS server. This number ranges from 0 to 100.

Default	2
Format	**`ip domain retry <`***`number`***`>`**
Mode	Global Config

no ip domain retry

Use this command to return to the default.

Format	**`no ip domain retry <`***`number`***`>`**
Mode	Global Config

ip domain timeout

Use this command to specify the amount of time to wait for a response to a DNS query. The parameter <*`seconds`*> specifies the time, in seconds, to wait for a response to a DNS query. <*`seconds`*> ranges from 0 to 3600.

Default	3
Format	**`ip domain timeout <`***`seconds`***`>`**
Mode	Global Config

no ip domain timeout

Use this command to return to the default setting.

Format	**`no ip domain timeout <`***`seconds`***`>`**
Mode	Global Config

clear host

Use this command to delete entries from the host name-to-address cache. This command clears the entries from the DNS cache maintained by the software. This command clears both IPv4 and IPv6 entries.

Format	**`clear host {<`***`name`***`>	all}`**
Mode	Privileged EXEC

Field	Description
name	A particular host entry to remove. <*name*> ranges from 1-255 characters.
all	Removes all entries.

show hosts

Use this command to display the default domain name, a list of name server hosts, the static and the cached list of host names and addresses <*name*> ranges from 1-255 characters. This command displays both IPv4 and IPv6 entries. ..

Format	**show hosts [***name***]**
Mode	User EXEC

Field	Description
Host Name	Domain host name.
Default Domain	Default domain name.
Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending Domain Name System (DNS) queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.

Example: The following shows example CLI display output for the command.

```
<Switch> show hosts

Host name......................... Device
Default domain.................... gm.com
Default domain list............... yahoo.com, Stanford.edu, rediff.com
Domain Name lookup................ Enabled
Number of retries................. 5
Retry timeout period.............. 1500
Name servers (Preference order)... 176.16.1.18 176.16.1.19


Configured host name-to-address mapping:

Host                           Addresses
------------------------------ ------------------------------
accounting.gm.com              176.16.8.8

Host             Total  Elapsed      Type      Addresses
--------------- -------- ------    --------     --------------
```

```
www.stanford.edu   72      3          IP        171.64.14.203
```

Packet Capture Commands

Packet capture commands assist in troubleshooting protocol-related problems with the management CPU. The packets to and from the management CPU can be captured in an internally allocated buffer area for export to a PC host for protocol analysis. Public domain packet analysis tools like Ethereal can be used to decode and review the packets in detail. Capturing can be performed in a variety of modes, either transmit-side only, receive-side only, or both. The number of packets captured will depend on the size of the captured packets.

capture transmit packet

This command enables the capturing of transmit packets.

Format	`capture transmit packet`
Mode	Global Config

no capture transmit packet

This command disables the capturing of transmit packets.

Format	`no capture transmit packet`
Mode	Global Config

capture receive packet

This command enables the capturing of receive packets.

Format	`capture receive packet`
Mode	Global Config

no capture receive packet

This command disables the capturing of receive packets.

Format	`no capture receive packet`
Mode	Global Config

capture all packets

This command enables the capturing of receive packets.

Format	`capture all packet`
Mode	Global Config

no capture all packets

This command disables the capturing of all packets.

Format	`no capture all packets`
Mode	Global Config

capture wrap

This command enables the Buffer Wrapping configuration. Once the capture buffer is full, writes to the buffer will wrap around to allow continuous packet capture.

Format	`capture wrap`
Mode	Global Config
Default	Enabled

show capture packets

This command displays packets being captured from the buffer. The output of the show command can be redirected to a text file. The resultant text file can be fed to the **text2pcap** utility or the Ethereal public domain packet analyzer, which can then be translated to a cap file.

Format	`show capture packets`

Mode	Global Config
Default	Enabled

Serviceability Packet Tracing Commands

These commands improve the capability of network engineers to diagnose conditions affecting their managed switch product.

⚠	**Caution!** The output of “debug” commands can be long and may adversely affect system performance.

debug arp

Use this command to enable ARP debug protocol messages.

Default	disabled
Format	`debug arp`
Mode	Privileged EXEC

no debug arp

Use this command to disable ARP debug protocol messages.

Format	`no debug arp`
Mode	Privileged EXEC

debug auto-voip

Use this command to enable Auto VOIP debug messages. Use the optional parameters to trace H323, SCCP, or SIP packets respectively.

Default	disabled
Format	`debug auto-voip [H323|SCCP|SIP]`
Mode	Privileged EXEC

no debug auto-voip

Use this command to disable Auto VOIP debug messages.

Format	`no debug auto-voip`
Mode	Privileged EXEC

debug clear

This command disables all previously enabled “debug” traces.

Default	disabled
Format	`debug clear`
Mode	Privileged EXEC

debug console

This command enables the display of “debug” trace output on the login session in which it is executed. Debug console display must be enabled in order to view any trace output. The output of debug trace commands will appear on all login sessions for which debug console has been enabled. The configuration of this command remains in effect for the life of the login session. The effect of this command is not persistent across resets.

Default	disabled
Format	`debug console`
Mode	Privileged EXEC

no debug console

This command disables the display of “debug” trace output on the login session in which it is executed.

Format	`no debug console`
Mode	Privileged EXEC

debug dot1x packet

Use this command to enable dot1x packet debug trace.

Default	disabled
Format	`debug dot1x`
Mode	Privileged EXEC

no debug dot1x packet

Use this command to disable dot1x packet debug trace.

Format	`no debug dot1x`
Mode	Privileged EXEC

debug igmpsnooping packet

This command enables tracing of IGMP Snooping packets received and transmitted by the switch.

Default	disabled
Format	`debug igmpsnooping packet`
Mode	Privileged EXEC

no debug igmpsnooping packet

This command disables tracing of IGMP Snooping packets.

Format	`no debug igmpsnooping packet`
Mode	Privileged EXEC

debug igmpsnooping packet transmit

This command enables tracing of IGMP Snooping packets transmitted by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet transmit`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt TX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac:
00:03:0e:00:00:00 Dest_Mac: 01:00:5e:00:00:01 Src_IP: 9.1.1.1 Dest_IP: 225.0.0.1
Type: V2_Membership_Report Group: 225.0.0.1
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the IP header in the packet.
Dest_IP	The destination multicast IP address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • `Membership Query` – IGMP Membership Query • `V1_Membership_Report` – IGMP Version 1 Membership Report • `V2_Membership_Report` – IGMP Version 2 Membership Report • `V3_Membership_Report` – IGMP Version 3 Membership Report • `V2_Leave_Group` – IGMP Version 2 Leave Group
Group	Multicast group address in the IGMP header.

no debug igmpsnooping transmit

This command disables tracing of transmitted IGMP snooping packets.

Format	`no debug igmpsnooping transmit`
Mode	Privileged EXEC

debug igmpsnooping packet receive

This command enables tracing of IGMP Snooping packets received by the switch. Snooping should be enabled on the device and the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug igmpsnooping packet receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 02:45:06 192.168.17.29-1 IGMPSNOOP[185429992]:
igmp_snooping_debug.c(116) 908 % Pkt RX - Intf: 1/0/20(20), Vlan_Id:1 Src_Mac:
00:03:0e:00:00:10 Dest_Mac: 01:00:5e:00:00:05 Src_IP: 11.1.1.1 Dest_IP: 225.0.0.5
Type: Membership_Query Group: 225.0.0.5
```

The following parameters are displayed in the trace message:

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_Mac	Source MAC address of the packet.
Dest_Mac	Destination multicast MAC address of the packet.
Src_IP	The source IP address in the ip header in the packet.
Dest_IP	The destination multicast ip address in the packet.
Type	The type of IGMP packet. Type can be one of the following: • `Membership_Query` – IGMP Membership Query • `V1_Membership_Report` – IGMP Version 1 Membership Report • `V2_Membership_Report` – IGMP Version 2 Membership Report • `V3_Membership_Report` – IGMP Version 3 Membership Report • `V2_Leave_Group` – IGMP Version 2 Leave Group

Parameter	Definition
Group	Multicast group address in the IGMP header.

no debug igmpsnooping receive

This command disables tracing of received IGMP Snooping packets.

Format	`no debug igmpsnooping receive`
Mode	Privileged EXEC

debug ip acl

Use this command to enable debug of IP Protocol packets matching the ACL criteria.

Default	disabled
Format	`debug ip acl <acl Number>`
Mode	Privileged EXEC

no debug ip acl

Use this command to disable debug of IP Protocol packets matching the ACL criteria.

Format	`no debug ip acl <acl Number>`
Mode	Privileged EXEC

debug ip dvmrp packet

Use this command to trace DVMRP packet reception and transmission. **receive** traces only received DVMRP packets and **transmit** traces only transmitted DVMRP packets. When neither keyword is used in the command, then all DVMRP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console

Default	disabled
Format	`debug ip dvmrp packet [receive|transmit]`
Mode	Privileged EXEC

no debug ip dvmrp packet

Use this command to disable debug tracing of DVMRP packet reception and transmission.

Format	`no debug ip dvmrp packet [receive|transmit]`
Mode	Privileged EXEC

debug ip igmp packet

Use this command to trace IGMP packet reception and transmission. **receive** traces only received IGMP packets and **transmit** traces only transmitted IGMP packets. When neither keyword is used in the command, then all IGMP packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ip igmp packet [receive|transmit]`
Mode	Privileged EXEC

no debug ip igmp packet

Use this command to disable debug tracing of IGMP packet reception and transmission.

Format	`no debug ip igmp packet [receive|transmit]`
Mode	Privileged EXEC

debug ip mcache packet

Use this command for tracing MDATA packet reception and transmission. **receive** traces only received data packets and **transmit** traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled

Format	`debug ip mcache packet [receive|transmit]`
Mode	Privileged EXEC

no debug ip mcache packet

Use this command to disable debug tracing of MDATA packet reception and transmission.

Format	`no debug ip mcache packet [receive|transmit]`
Mode	Privileged EXEC

debug ip pimdm packet

Use this command to trace PIMDM packet reception and transmission. **receive** traces only received PIMDM packets and **transmit** traces only transmitted PIMDM packets. When neither keyword is used in the command, then all PIMDM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ip pimdm packet [receive|transmit]`
Mode	Privileged EXEC

no debug ip pimdm packet

Use this command to disable debug tracing of PIMDM packet reception and transmission.

Format	`no debug ip pimdm packet [receive|transmit]`
Mode	Privileged EXEC

debug ip pimsm packet

Use this command to trace PIMSM packet reception and transmission. **receive** traces only received PIMSM packets and **transmit** traces only transmitted PIMSM packets. When neither keyword is used in the command, then all PIMSM packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ip pimsm packet [receive|transmit]`
Mode	Privileged EXEC

no debug ip pimsm packet

Use this command to disable debug tracing of PIMSM packet reception and transmission.

Format	`no debug ip pimsm packet [receive|transmit]`
Mode	Privileged EXEC

debug ip vrrp

Use this command to enable VRRP debug protocol messages.

Default	disabled
Format	`debug ip vrrp`
Mode	Privileged EXEC

no debug ip vrrp

Use this command to disable VRRP debug protocol messages.

Format	`no debug ip vrrp`
Mode	Privileged EXEC

debug ipv6 mcache packet

Use this command for tracing MDATAv6 packet reception and transmission. **receive** traces only received data packets and **transmit** traces only transmitted data packets. When neither keyword is used in the command, then all data packet traces are dumped. Vital information such as source address, destination address, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ipv6 mcache packet [receive|transmit]`
Mode	Privileged EXEC

no debug ipv6 mcache packet

Use this command to disable debug tracing of MDATAv6 packet reception and transmission.

Format	`no debug ipv6 mcache packet [receive|transmit]`
Mode	Privileged EXEC

debug ipv6 mld packet

Use this command to trace MLDv6 packet reception and transmission. **receive** traces only received MLDv6 packets and **transmit** traces only transmitted MLDv6 packets. When neither keyword is used in the command, then all MLDv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ipv6 mld packet [receive|transmit]`
Mode	Privileged EXEC

no debug ipv6 mld packet

Use this command to disable debug tracing of MLDv6 packet reception and transmission.

Format	`no debug ipv6 mld packet [receive|transmit]`
Mode	Privileged EXEC

debug ipv6 pimdm packet

Use this command to trace PIMDMv6 packet reception and transmission. **receive** traces only received PIMDMv6 packets and **transmit** traces only transmitted PIMDMv6 packets. When neither keyword is used in the command, then all PIMDMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ipv6 pimdm packet [receive|transmit]`
Mode	Privileged EXEC

no debug ipv6 pimdm packet

Use this command to disable debug tracing of PIMDMv6 packet reception and transmission.

debug ipv6 pimsm packet

Use this command to trace PIMSMv6 packet reception and transmission. **receive** traces only received PIMSMv6 packets and **transmit** traces only transmitted PIMSMv6 packets. When neither keyword is used in the command, then all PIMSMv6 packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug ipv6 pimsm packet [receive|transmit]`
Mode	Privileged EXEC

no debug ipv6 pimsm packet

Use this command to disable debug tracing of PIMSMv6 packet reception and transmission.

Format	`no debug ipv6 pimsm packet [receive|transmit]`
Mode	Privileged EXEC

debug lacp packet

This command enables tracing of LACP packets received and transmitted by the switch.

Default	disabled
Format	`debug lacp packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 14:04:51 10.254.24.31-1 DOT3AD[183697744]: dot3ad_debug.c(385) 58 %%
 Pkt TX - Intf: 1/0/1(1), Type: LACP, Sys: 00:11:88:14:62:e1, State: 0x47, Key:
0x36
```

no debug lacp packet

This command disables tracing of LACP packets.

Format	`no debug lacp packet`
Mode	Privileged EXEC

debug mldsnooping packet

Use this command to trace MLD snooping packet reception and transmission. **receive** traces only received MLD snooping packets and **transmit** traces only transmitted MLD snooping packets. When neither keyword is used in the command, then all MLD snooping packet traces are dumped. Vital information such as source address, destination address, control packet type, packet length, and the interface on which the packet is received or transmitted is displayed on the console.

Default	disabled
Format	`debug mldsnooping packet [receive|transmit]`
Mode	Privileged EXEC

no debug mldsnooping packet

Use this command to disable debug tracing of MLD snooping packet reception and transmission.

debug ospf packet

This command enables tracing of OSPF packets received and transmitted by the switch.

Default	disabled
Format	`debug ospf packet`
Mode	Privileged EXEC

Sample outputs of the trace messages are shown below.

```
<15> JAN 02 11:03:31 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25430 % Pkt
RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:224.0.0.5 AreaId:0.0.0.0 Type:HELLO NetMask:255.255.255.0
DesigRouter:0.0.0.0 Backup:0.0.0.0

<15> JAN 02 11:03:35 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25431 % Pkt
TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:DB_DSCR Mtu:1500 Options:E
Flags: I/M/MS Seq:126166

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(297) 25434 % Pkt
RX - Intf:2/0/48 Src
Ip:192.168.50.2 DestIp:192.168.50.1 AreaId:0.0.0.0 Type:LS_REQ Length: 1500

<15> JAN 02 11:03:36 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25435 % Pkt
TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:192.168.50.2 AreaId:0.0.0.0 Type:LS_UPD Length: 1500

<15> JAN 02 11:03:37 10.50.50.1-2 OSPF[46300472]: ospf_debug.c(293) 25441 % Pkt
TX - Intf:2/0/48 Src
Ip:10.50.50.1 DestIp:224.0.0.6 AreaId:0.0.0.0 Type:LS_ACK Length: 1500
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.

Parameter	Definition
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number).
SrcIp	The source IP address in the IP header of the packet.
DestIp	The destination IP address in the IP header of the packet.
AreaId	The area ID in the OSPF header of the packet.
Type	Could be one of the following: `HELLO` – Hello packet `DB_DSCR` – Database descriptor `LS_REQ` – LS Request `LS_UPD` – LS Update `LS_ACK` – LS Acknowledge

The remaining fields in the trace are specific to the type of OSPF Packet.

HELLO packet field definitions:

Parameter	Definition
Netmask	The netmask in the hello packet.
DesignRouter	Designated Router IP address.
Backup	Backup router IP address.

DB_DSCR packet field definitions:

Field	Definition
MTU	MTU
Options	Options in the OSPF packet.
Flags	Could be one or more of the following: • `I` – Init • `M` – More • `MS` – Master/Slave
Seq	Sequence Number of the DD packet.

LS_REQ packet field definitions.

Field	Definition
Length	Length of packet

LS_UPD packet field definitions.

Field	Definition
Length	Length of packet

LS_ACK packet field definitions.

Field	Definition
Length	Length of packet

no debug ospf packet

This command disables tracing of OSPF packets.

Format	`no debug ospf packet`
Mode	Privileged EXEC

debug ospfv3 packet

Use this command to enable OSPFv3 packet debug trace.

Default	disabled
Format	`debug ospfv3 packet`
Mode	Privileged EXEC

no debug ospfv3 packet

Use this command to disable tracing of OSPFv3 packets.

Format	`no debug ospfv3 packet`
Mode	Privileged EXEC

debug ping packet

This command enables tracing of ICMP echo requests and responses. The command traces pings on the network port/ serviceport for switching packages. For routing packages, pings are traced on the routing ports as well.

Default	disabled
Format	`debug ping packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:21:22 192.168.17.29-1 SIM[181040176]: sim_debug.c(128) 20 % Pkt TX
- Intf: 1/0/1(1),
SRC_IP:10.50.50.2, DEST_IP:10.50.50.1, Type:ECHO_REQUEST


<15> JAN 01 00:21:22 192.168.17.29-1 SIM[182813968]: sim_debug.c(82) 21 % Pkt RX
- Intf: 1/0/1(1), S
RC_IP:10.50.50.1, DEST_IP:10.50.50.2, Type:ECHO_REPLY
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
SRC_IP	The source IP address in the IP header in the packet.
DEST_IP	The destination IP address in the IP header in the packet.
Type	Type determines whether or not the ICMP message is a REQUEST or a RESPONSE.

no debug ping packet

This command disables tracing of ICMP echo requests and responses.

Format	`no debug ping packet`
Mode	Privileged EXEC

debug rip packet

This command turns on tracing of RIP requests and responses. This command takes no options. The output is directed to the log file.

Default	disabled
Format	`debug rip packet`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 00:35:15 192.168.17.29-1 RIP[181783160]: rip_map_debug.c(96) 775 %
Pkt RX on Intf: 1/0/1(1), Src_IP:43.1.1.1 Dest_IP:43.1.1.2
Rip_Version: RIPv2 Packet_Type:RIP_RESPONSE
ROUTE 1): Network: 10.1.1.0 Mask: 255.255.255.0 Metric: 1
ROUTE 2): Network: 40.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 3): Network: 10.50.50.0 Mask: 255.255.255.0 Metric: 1
ROUTE 4): Network: 41.1.0.0 Mask: 255.255.0.0 Metric: 1
ROUTE 5): Network:42.0.0.0 Mask:255.0.0.0 Metric:1
Another 6 routes present in packet not displayed.
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX/RX	TX refers to a packet transmitted by the device. RX refers to packets received by the device.
Intf	The interface that the packet came in or went out on. Format used is unit/slot/port (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Src_IP	The source IP address in the IP header of the packet.
Dest_IP	The destination IP address in the IP header of the packet.
Rip_Version	RIP version used <RIPv1 or RIPv2>.
Packet_Type	Type of RIP packet. <RIP_REQUEST or RIP_RESPONSE>.
Routes	Up to 5 routes in the packet are displayed in the following format: Network: <a.b.c.d> Mask <a.b.c.d> Next_Hop <a.b.c.d> Metric <a> The next hop is only displayed if it is different from `0.0.0.0`. For RIPv1 packets, Mask is always `0.0.0.0`.
Number of routes not printed	Only the first five routes present in the packet are included in the trace. There is another notification of the number of additional routes present in the packet that were not included in the trace.

no debug rip packet

This command disables tracing of RIP requests and responses.

Format	`no debug rip packet`
Mode	Privileged EXEC

debug sflow packet

Use this command to enable sFlow debug packet trace.

Default	disabled
Format	`debug sflow packet`
Mode	Privileged EXEC

no debug sflow packet

Use this command to disable sFlow debug packet trace.

Format	`no debug sflow packet`
Mode	Privileged EXEC

debug spanning-tree bpdu

This command enables tracing of spanning tree BPDUs received and transmitted by the switch.

Default	disabled
Format	`debug spanning-tree bpdu`
Mode	Privileged EXEC

no debug spanning-tree bpdu

This command disables tracing of spanning tree BPDUs.

Format	`no debug spanning-tree bpdu`
Mode	Privileged EXEC

debug spanning-tree bpdu receive

This command enables tracing of spanning tree BPDUs received by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets for a particular interface.

Default	disabled
Format	`debug spanning-tree bpdu receive`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 %
Pkt RX - Intf: 1/0/9(9), Source_Mac: 00:11:88:4e:c2:10 Version: 3, Root Mac:
00:11:88:4e:c2:00, Root Priority: 0x8000 Path Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	Definition
RX	A packet received by the device.
Intf	The interface that the packet came in on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu receive

This command disables tracing of received spanning tree BPDUs.

Format	`no debug spanning-tree bpdu receive`
Mode	Privileged EXEC

debug spanning-tree bpdu transmit

This command enables tracing of spanning tree BPDUs transmitted by the switch. Spanning tree should be enabled on the device and on the interface in order to monitor packets on a particular interface.

Default	disabled
Format	`debug spanning-tree bpdu transmit`
Mode	Privileged EXEC

A sample output of the trace message is shown below.

```
<15> JAN 01 01:02:04 192.168.17.29-1 DOT1S[191096896]: dot1s_debug.c(1249) 101 %
Pkt TX - Intf: 1/0/7(7), Source_Mac: 00:11:88:4e:c2:00 Version: 3, Root_Mac:
00:11:88:4e:c2:00, Root_Priority: 0x8000 Path_Cost: 0
```

The following parameters are displayed in the trace message:

Parameter	Definition
TX	A packet transmitted by the device.
Intf	The interface that the packet went out on. Format used is unit/port/slot (internal interface number). Unit is always shown as 1 for interfaces on a non-stacking device.
Source_Mac	Source MAC address of the packet.
Version	Spanning tree protocol version (0-3). 0 refers to STP, 2 RSTP and 3 MSTP.
Root_Mac	MAC address of the CIST root bridge.
Root_Priority	Priority of the CIST root bridge. The value is between 0 and 61440. It is displayed in hex in multiples of 4096.
Path_Cost	External root path cost component of the BPDU.

no debug spanning-tree bpdu transmit

This command disables tracing of transmitted spanning tree BPDUs.

Format	`no debug spanning-tree bpdu transmit`
Mode	Privileged EXEC

Cable Test Command

The cable test feature enables you to determine the cable connection status on a selected port.

> **Note:** The cable test feature is supported only for copper cable. It is not supported for optical fiber cable. If the port has an active link while the cable test is run, the link can go down for the duration of the test.

cablestatus

This command returns the status of the specified port.

Format	**`cablestatus`** *`<unit/slot/port>`*
Mode	Privileged EXEC

Field	**Description**
Cable Status	One of the following statuses is returned: • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Short**: There is an electrical short in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working.

Field	Description
Cable Length	If this feature is supported by the PHY for the current link speed, the cable length is displayed as a range between the shortest estimated length and the longest estimated length. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded. Unknown is displayed if the cable length could not be determined.

sFlow Commands

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

sflow receiver

Use this command to configure the sFlow collector parameters (owner string, receiver timeout, max datagram size, IP address, and port).

Format

```
sflow receiver <rcvr_idx> owner <owner-string> timeout <rcvr_timeout>
max datagram <size> ip/ipv6 <ip> port <port>
```

Mode Global Config

Field	Description
Receiver Owner	The identity string for the receiver, the entity making use of this sFlowRcvrTable entry. The range is 127 characters. The default is a null string. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string to a non-null value. The entry must be claimed before assigning a receiver to a sampler or poller.
Receiver Timeout	The time, in seconds, remaining before the sampler or poller is released and stops sending samples to receiver. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0-4294967295 seconds. The default is zero (0).

Field	Description
Receiver Max Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The management entity should set this value to avoid fragmentation of the sFlow datagrams. The allowed range is 200 to 9116). The default is 1400.
Receiver IP	The sFlow receiver IP address. If set to 0.0.0.0, no sFlow datagrams will be sent. The default is 0.0.0.0.
Receiver Port	The destination Layer4 UDP port for sFlow datagrams. The range is 1-65535. The default is 6343.

no sflow receiver

Use this command to set the sFlow collector parameters back to the defaults.

Format `no sflow receiver <indx> {ip <ip-address> | maxdatagram <size> | owner <string> timeout <interval> | port <14-port>}`

Mode Global Config

sflow sampler

A data source configured to collect flow samples is called a poller. Use this command to configure a new sFlow sampler instance for this data source if <*rcvr_idx*> is valid.

Format `sflow sampler {<rcvr-indx> | rate <sampling-rate> | maxheadersize <size>}`

Mode Interface Config

Field	Description
Receiver Index	The sFlow Receiver for this sFlow sampler to which flow samples are to be sent. A value of zero (0) means that no receiver is configured, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. Possible values are 1-8. The default is 0.
Maxheadersize	The maximum number of bytes that should be copied from the sampler packet. The range is 20-256. The default is 128. When set to zero (0), all the sampler parameters are set to their corresponding default value.

Field	Description
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of 1 counts all packets. A value of zero (0) disables sampling. A value of N means that out of N incoming packets, 1 packet will be sampled. The range is 1024-65536 and 0. The default is 0.

no sflow sampler

Use this command to reset the sFlow sampler instance to the default settings.

Format	`no sflow sampler {<`*`rcvr-indx`*`> | rate <`*`sampling-rate`*`> | maxheadersize <`*`size`*`>}`
Mode	Interface Config

sflow poller

A data source configured to collect counter samples is called a poller. Use this command to enable a new sFlow poller instance for this data source if <*rcvr_idx*> is valid.

Format	`sflow poller {<rcvr-indx> | interval <poll-interval>}`
Mode	Interface Config

Field	Description
Receiver Index	Enter the sFlow Receiver associated with the sampler/poller. A value of zero (0) means that no receiver is configured. The range is 1-8. The default is 0.
Poll Interval	Enter the sFlow instance polling interval. A poll interval of zero (0) disables counter sampling. When set to zero (0), all the poller parameters are set to their corresponding default value. The range is 0-86400. The default is 0. A value of N means once in N seconds a counter sample is generated.

no sflow poller

Use this command to reset the sFlow poller instance to the default settings.

Format `no sflow poller {<rcvr-indx> | interval <poll-interval>}`

Mode Interface Config

show sflow agent

The sFlow agent collects time-based sampling of network interface statistics and flow-based samples. These are sent to the configured sFlow receivers. Use this command to display the sFlow agent information.

Format `show sflow agent`

Mode Privileged EXEC

Field	Description
sFlow Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version; Organization; Software Revision where: • MIB Version: ‘1.3’, the version of this MIB. • Organization: Netgear. • Revision: 1.0
IP Address	The IP address associated with this agent.

Example: The following shows example CLI display output for the command.

```
(switch) #show sflow agent

sFlow Version.................................. 1.3;Netgear;1.0
IP Address..................................... 10.131.12.66
```

show sflow pollers

Use this command to display the sFlow polling instances created on the switch. Use “-” for range.

Format `show sflow pollers`

Mode Privileged EXEC

Field	Description
Poller Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver associated with this sFlow counter poller.
Poller Interval	The number of seconds between successive samples of the counters associated with this data source.

show sflow receivers

Use this command to display configuration information related to the sFlow receivers.

Format	`show sflow receivers [<index>]`
Mode	Privileged EXEC

Field	Description
Receiver Index	The sFlow Receiver associated with the sampler/poller.
Owner String	The identity string for receiver, the entity making use of this sFlowRcvrTable entry.
Time Out	The time (in seconds) remaining before the receiver is released and stops sending samples to sFlow receiver.
Max Datagram Size	The maximum number of bytes that can be sent in a single sFlow datagram.
Port	The destination Layer4 UDP port for sFlow datagrams.
IP Address	The sFlow receiver IP address.
Address Type	The sFlow receiver IP address type. For an IPv4 address, the value is 1 and for an IPv6 address, the value is 2.
Datagram Version	The sFlow protocol version to be used while sending samples to sFlow receiver.

Example: The following shows example CLI display output for the command.

```
(switch) #show sflow receivers 1
Receiver Index................................ 1
Owner String..................................
Time out...................................... 0
IP Address:................................... 0.0.0.0
Address Type.................................. 1
Port.......................................... 6343
```

```
Datagram Version.............................. 5
Maximum Datagram Size......................... 1400
```

show sflow samplers

Use this command to display the sFlow sampling instances created on the switch.

Format	`show sflow samplers`
Mode	Privileged EXEC

Field	Description
Sampler Data Source	The sFlowDataSource (slot/port) for this sFlow sampler. This agent will support Physical ports only.
Receiver Index	The sFlowReceiver configured for this sFlow sampler.
Packet Sampling Rate	The statistical sampling rate for packet sampling from this source.
Max Header Size	The maximum number of bytes that should be copied from a sampled packet to form a flow sample.

Software License Commands

Release 9.0 allows the XSM7224S to be licensed such that this switch can configure advanced features.

The following table lists the software license matrix for the XSM7224S:

Switch	IPv4 Routing	IPv6 Routing	IP Multicast
XSM7224S	Licensed	Licensed	Licensed

Note: The software license will allow the user to download a license file only on the Master unit. The file cannot be downloaded on a Slave unit.

Note: There are two options to download the license file to the switch:
1). Use the command **Copy** to download the license file through the CLI.
2). Go to the **Maintenance** > **Download** page to download the licence file through the GUI.

show license

This command displays the license status.

License Date indicates the date of the license. License Status indicates whether license is active or inactive.

Format	`show license`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(XSM7224S) #show license
License date : Apr-9-2010
License copy : 1
License Status: Active
Description : License key is active.
(XSM7224S) #
```

show license features

This command displays the features that are licensed on the switch

Format	`show license features`
Mode	Privileged EXEC

Example: The following shows example CLI display output for the command.

```
(XSM7224S) #show license features
IGMP
MCAST
PIMDM
DVMRP
PIMSM
OSPFV3
IPV6
```

IP Address Conflict Commands

ip address-conflict-detect run

This command triggers the switch to run active address conflict detection by sending gratuitous ARP packets for IPv4 addresses on the switch.

Format	`ip address-conflict-detect run`
Mode	Global Config

show ip address-conflict

This command displays the status information corresponding to the last detected address conflict.

Term	Definition
Address Conflict Detection Status	Identifies whether the switch has detected an address conflict on any IP address.
Last Conflicting IP Address	The IP Address that was last detected as conflicting on any interface.
Last Conflicting MAC Address	The MAC Address of the conflicting host that was last detected on any interface.
Time Since Conflict Detected	The time in days, hours, minutes and seconds since the last address conflict was detected.

clear ip address-conflict-detect

This command clears the detected address conflict status information.

Format	`clear ip address-conflict-detect`
Mode	Privileged EXEC

Link Local Protocol Filtering Commands

Link Local Protocol Filtering (LLPF) allows the switch to filter out multiple proprietary protocol PDUs, such as Port Aggregation Protocol (PAgP), if the problems occur with proprietary protocols running on standards-based switches. If certain protocol PDUs cause unexpected results, LLPF can be enabled to prevent those protocol PDUs from being processed by the switch.

llpf blockall

Use this command to block LLPF protocol(s) on a port. Use `blockall` to filter all PDUs with a DMAC of 01:00:00:0C:CC:CX on the interface. Use `blockisdp` to filter the ISDP packets on the interface. Use `blockvtp` to filter the VTP packets on the interface. Use `blockdtp` to filter the DTP packets on the interface. Use `blockudld` to filter the UDLD packets on the interface. Use `blockpagp` to filter the PAGP packets on the interface. Use `blocksstp` to filter the SSTP packets on the interface.

Format	`llpf {blockisdp | blockvtp | blockdtp | blockudld | blockpagp | blocksstp | blockall }`
Mode	Interface Config
Default	Disable

no llpf

Use this command to unblock LLPF protocol(s) on a port.

show llpf interface all

Use this command to display the status of LLPF rules configured on a particular port or on all ports.

Format	`show llpf interface [all | unit/slot/port]`
Mode	Privileged EXEC

Term	Definition
Block ISDP	Shows whether the port blocks ISDP PDUs.
Block VTP	Shows whether the port blocks VTP PDUs.
Block DTP	Shows whether the port blocks DTP PDUs.
Block UDLD	Shows whether the port blocks UDLD PDUs.
Block PAGP	Shows whether the port blocks PAGP PDUs.
Block SSTP	Shows whether the port blocks SSTP PDUs.
Block All	Shows whether the port blocks all proprietary PDUs available for the LLDP feature.

Chapter 7
Management Commands

This chapter describes the management commands available in the managed switch CLI.

The Management Commands chapter contains the following sections:

- "Configuring the Switch Management CPU" on page 7-2.
- "Network Interface Commands" on page 7-4.
- "Console Port Access Commands" on page 7-8.
- "Telnet Commands" on page 7-11.
- "Secure Shell (SSH) Commands" on page 7-16.
- "Management Security Commands" on page 7-19.
- "Hypertext Transfer Protocol (HTTP) Commands" on page 7-20.
- "Access Commands" on page 7-28.
- "User Account Commands" on page 7-29.
- "aaa ias-user username" on page 7-46.
- "RADIUS Commands" on page 7-59.
- "TACACS+ Commands" on page 7-73.
- "Configuration Scripting Commands" on page 7-77.
- "Pre-login Banner and System Prompt Commands" on page 7-79.
- "Switch Database Management (SDM) Templates" on page 7-80.

> ⚠ **Warning:** The commands in this chapter are in one of three functional groups:
>
> - Show commands display switch settings, statistics, and other information.
> - Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
> - Clear commands clear some or all of the settings to factory defaults.

Configuring the Switch Management CPU

To manage the switch via the web GUI or telnet, an IP address needs to be assigned to the switch management CPU. Whereas there are CLI commands that can be used to do this, **ezconfig** simplifies the task. The tool is applicable to all NETGEAR 7000-series managed switches, and allows you to configure the following parameters:

1. The administrator's user password and administrator-enable password
2. Management CPU IP address and network mask
3. System name and location information

The tool is interactive and uses questions to guide you through the steps required to perform its task. At the end of the session, it will ask you if you want to save the changed information. To see exactly what has been changed by ezconfig at the end of the session, use the **show running-config** command.

To perform any switch configuration other than the items listed above, use other CLI commands or the Web GUI.

ezconfig

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

Format	`ezconfig`
Mode	Privileged EXEC

The following is an example of an **ezconfig** session.

```
NETGEAR EZ Configuration Utility
--------------------------------
Hello and Welcome!

This utility will walk you thru assigning the IP address for the switch
management CPU. It will allow you to save the changes at the end. After
the session, simply use the newly assigned IP address to access the Web
GUI using any public domain Web browser.


Admin password not defined. Do you want to change the password?
(Y/N/Q)  y
Enter new password:********
Confirm new password:********
Password Changed!

The 'enable' password required for switch configuration via the command
line interface is currently not configured. Do you wish to change it (Y/N/
Q)?  y

Enter new password:********
Confirm new password:********
Password Changed!

Assigning an IP address to your switch management

Current IP Address Configuration
--------------------------------
IP address: 0.0.0.0
Subnet mask: 0.0.0.0
Gateway address: 0.0.0.0

Would you like to assign an IP address now (Y/N/Q)?  y

IP Address: 10.10.10.1
Subnet mask: 255.255.255.0
Gateway address: 10.10.10.10

Do you want to assign switch name and location information (Y/N/Q)?   y

System Name: testunit1
System Location: testlab
System Contact: Bud Lightyear
```

```
There are changes detected, do you wish to save the changes permanently
(Y/N)?  y

The configuration changes have been saved succesfully.  Please enter 'show
running-config' to see the final configuration.

Thanks for using EzConfig!
```

Network Interface Commands

This section describes the commands you use to configure a logical interface for management access. To configure the management VLAN, see "network mgmt_vlan" on page 3-32.

enable (Privileged EXEC access)

This command gives you access to the Privileged EXEC mode. From the Privileged EXEC mode, you can configure the network interface.

Format	`enable`
Mode	User EXEC

network parms

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet.

Format	`network parms` *`<ipaddr> <netmask> [<gateway>]`*
Mode	Privileged EXEC

network protocol

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the `bootp` parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the `dhcp` parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the `none` parameter, you must configure the network information for the switch manually.

Default	none
Format	`network protocol {none	bootp	dhcp}`
Mode	Privileged EXEC

network mac-address

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally administered (b'1').
- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or a group address (b'1').
- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format	`network mac-address <macaddr>`
Mode	Privileged EXEC

network mac-type

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default	burnedin
Format	`network mac-type {local	burnedin}`
Mode	Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format	`no network mac-type`
Mode	Privileged EXEC

network javamode

This command specifies whether or not the switch should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

Default	enabled
Format	`network javamode`
Mode	Privileged EXEC

no network javamode

This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

Format	`no network javamode`
Mode	Privileged EXEC

show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether or not any member ports are up; therefore, the show network command will always show “Interface Status” as “Up”.

Format	`show network`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Interface Status	The network interface status; it is always considered to be “up”.
IP Address	The IP address of the interface. The factory default value is 0.0.0.0.
Subnet Mask	The IP subnet mask for this interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for this IP interface. The factory default value is 0.0.0.0.
IPv6 Administrative Mode	Whether enabled or disabled.
IPv6 Address/ Length	The IPv6 address and length.
IPv6 Default Router	The IPv6 default router address.
Burned In MAC Address	The burned in MAC address used for in-band connectivity.
Locally Administered MAC Address	If desired, a locally administered MAC address can be configured for in-band connectivity. To take effect, 'MAC Address Type' must be set to 'Locally Administered'. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 should have the following mask 'xxxx xx10'. The MAC address used by this bridge when it must be referred to in a unique fashion. It is recommended that this be the numerically smallest MAC address of all ports that belong to this bridge. However it is only required to be unique. When concatenated with dot1dStpPriority a unique BridgeIdentifier is formed which is used in the Spanning Tree Protocol.
MAC Address Type	The MAC address which should be used for in-band connectivity. The choices are the burned in or the Locally Administered address. The factory default is to use the burned in MAC address.

The following shows example CLI display output for the network port.

```
(Netgear Switch) #show network

Interface Status............................... Always Up
IP Address..................................... 10.250.3.1
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.250.3.3
IPv6 Administrative Mode....................... Enabled
IPv6 Address/Length is ........................ FE80::210:18FF:FE82:337/64
IPv6 Address/Length is ........................ 3099::1/64
IPv6 Address/Length is ........................ 3099::210:18FF:FE82:337/64
IPv6 Default Router is ........................ FE80::204:76FF:FE73:423A
Burned In MAC Address.......................... 00:10:18:82:03:37
Locally Administered MAC Address............... 00:00:00:00:00:00
MAC Address Type............................... Burned In
Network Configuration Protocol Current......... None
```

```
Management VLAN ID............................ 1
Web Mode...................................... Enable
Java Mode..................................... Enable
```

Console Port Access Commands

This section describes the commands you use to configure the console port. You can use a serial cable to connect a management host directly to the console port of the switch.

configuration

This command gives you access to the Global Config mode. From the Global Config mode, you can configure a variety of system settings, including user accounts. From the Global Config mode, you can enter other command modes, including Line Config mode.

Format	`configuration`
Mode	Privileged EXEC

line

This command gives you access to the Line Config mode, which allows you to configure various Telnet settings, ssh settings, and the console port.

Format	`line {console | telnet | ssh}`
Mode	Global Config

serial baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Default	9600
Format	`serial baudrate` *`{1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}`*
Mode	Line Config

no serial baudrate

This command sets the communication rate of the terminal interface.

Format	`no serial baudrate`
Mode	Line Config

serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default	5
Format	`serial timeout <0-160>`
Mode	Line Config

no serial timeout

This command sets the maximum connect time (in minutes) without console activity.

Format	`no serial timeout`
Mode	Line Config

login authentication

To specify login authentication method list for remote telnet or console, use the `login authentication` command in line configuration mode.

Format	`login authentication {default | list-name}`
Mode	Line Config

no login authentication

To return to the default specified by the `login authentication` command.

Format	`no login authentication {default | list-name}`
Mode	Line Config

enable authentication

To specify authentication method list when the user accesses a higher privilege level in remote telnet or console, use the `enable authentication` command in line configuration mode.

Format	`enable authentication {default	*list-name*}`
Mode	Line Config

no enable authentication

To return to the default specified by the `enable authentication` command.

Format	`no enable authentication {default	*list-name*}`
Mode	Line Config

show serial

This command displays serial communication settings for the switch.

Format	`show serial`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400,57600, and 115200 baud. The factory default is 9600 baud.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity Type	The Parity Method used on the Serial Port. The Parity Method is always None.

Telnet Commands

This section describes the commands you use to configure and view Telnet settings. You can use Telnet to manage the device from a remote management host.

ip telnet server enable

Use this command to enable Telnet connections to the system and to enable the Telnet Server Admin Mode. This command opens the Telnet listening port.

Default	enabled
Format	`ip telnet server enable`
Mode	Privileged EXEC

no ip telnet server enable

Use this command to disable Telnet access to the system and to disable the Telnet Server Admin Mode. This command closes the Telnet listening port and disconnects all open Telnet sessions.

Format	`no ip telnet server enable`
Mode	Privileged EXEC

telnet

This command establishes a new outbound Telnet connection to a remote host. The *host* value must be a valid IP address or host name. Valid values for *port* should be a valid decimal integer in the range of 0 to 65535, where the default value is 23. If `[debug]` is used, the current Telnet options enabled is displayed. The optional *line* parameter sets the outbound Telnet operational mode as ‘linemode’ where, by default, the operational mode is ‘character mode’. The *noecho* option disables local echo.

Format	`telnet <ip-address|hostname> <port> [debug] [line] [noecho]`
Modes	• Privileged EXEC • User EXEC

transport input telnet

This command regulates new Telnet sessions. If enabled, new Telnet sessions can be established until there are no more sessions available. An established session remains active until the session is ended or an abnormal network error ends the session.

Note: If the Telnet Server Admin Mode is disabled, Telnet sessions cannot be established. Use the `ip telnet server enable` command to enable Telnet Server Admin Mode.

Default	enabled
Format	`transport input telnet`
Mode	Line Config

no transport input telnet

Use this command to prevent new Telnet sessions from being established.

Format	`no transport input telnet`
Mode	Line Config

transport output telnet

This command regulates new outbound Telnet connections. If enabled, new outbound Telnet sessions can be established until the system reaches the maximum number of simultaneous outbound Telnet sessions allowed. An established session remains active until the session is ended or an abnormal network error ends it.

Default	enabled
Format	`transport output telnet`
Mode	Line Config

no transport output telnet

Use this command to prevent new outbound Telnet connection from being established.

Format	`no transport output telnet`
Mode	Line Config

session-limit

This command specifies the maximum number of simultaneous outbound Telnet sessions. A value of 0 indicates that no outbound Telnet session can be established.

Default	5
Format	`session-limit <0-5>`
Mode	Line Config

no session-limit

This command sets the maximum number of simultaneous outbound Telnet sessions to the default value.

Format	`no session-limit`
Mode	Line Config

session-timeout

This command sets the Telnet session timeout value.The timeout value unit of time is minutes.

Default	5
Format	`session-timeout <1-160>`
Mode	Line Config

no session-timeout

This command sets the Telnet session timeout value to the default. The timeout value unit of time is minutes.

Format	`no session-timeout`
Mode	Line Config

telnetcon maxsessions

This command specifies the maximum number of Telnet connection sessions that can be established. A value of 0 indicates that no Telnet connection can be established. The range is 0-5.

Default	4
Format	`telnetcon maxsessions <0-4>`
Mode	Privileged EXEC

no telnetcon maxsessions

This command sets the maximum number of Telnet connection sessions that can be established to the default value.

Format	`no telnetcon maxsessions`
Mode	Privileged EXEC

telnetcon timeout

This command sets the Telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

➡	**Note:** When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.

Default	5
Format	`telnetcon timeout <1-160>`
Mode	Privileged EXEC

no telnetcon timeout

This command sets the Telnet connection session timeout value to the default.

Note: Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

Format	`no telnetcon timeout`
Mode	Privileged EXEC

show telnet

This command displays the current outbound Telnet settings. In other words, these settings apply to Telnet connections initiated from the switch to a remote system.

Format	`show telnet`
Modes	• Privileged EXEC • User EXEC

Term	Definition
Outbound Telnet Login Timeout	The number of minutes an outbound Telnet session is allowed to remain inactive before being logged off.
Maximum Number of Outbound Telnet Sessions	The number of simultaneous outbound Telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound Telnet sessions will be allowed.

show telnetcon

This command displays the current inbound Telnet settings. In other words, these settings apply to Telnet connections initiated from a remote system to the switch.

Format	**`show telnetcon`**
Modes	• Privileged EXEC • User EXEC

Term	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from 1 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	New Telnet sessions will not be allowed when this field is set to no. The factory default value is yes.

Secure Shell (SSH) Commands

This section describes the commands you use to configure SSH access to the switch. Use SSH to access the switch from a remote management host.

Note: The system allows a maximum of 5 SSH sessions.

ip ssh

Use this command to enable SSH access to the system. (This command is the short form of the **`ip ssh server enable`** command.)

Default	disabled

Format	`ip ssh`
Mode	Privileged EXEC

ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

Default	1 and 2
Format	`ip ssh protocol` *`[1] [2]`*
Mode	Privileged EXEC

ip ssh server enable

This command enables the IP secure shell server.

Default	disabled
Format	`ip ssh server enable`
Mode	Privileged EXEC

no ip ssh server enable

This command disables the IP secure shell server.

Format	`no ip ssh server enable`
Mode	Privileged EXEC

sshcon maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Default	5
Format	`sshcon maxsessions <`*`0-5`*`>`
Mode	Privileged EXEC

no sshcon maxsessions

This command sets the maximum number of allowed SSH connection sessions to the default value.

Format	`no sshcon maxsessions`
Mode	Privileged EXEC

sshcon timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. The time is a decimal value from 1 to 160.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Default	5
Format	`sshcon timeout <1-160>`
Mode	Privileged EXEC

no sshcon timeout

This command sets the SSH connection session timeout value, in minutes, to the default.

Changing the timeout value for active sessions does not become effective until the session is re accessed. Also, any keystroke activates the new timeout duration.

Format	`no sshcon timeout`
Mode	Privileged EXEC

show ip ssh

This command displays the ssh settings.

Format	`show ip ssh`
Mode	Privileged EXEC

Term	Definition
Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
Protocol Level	The protocol level may have the values of version 1, version 2 or both versions 1 and version 2.
SSH Sessions Currently Active	The number of SSH sessions currently active.
Max SSH Sessions Allowed	The maximum number of SSH sessions allowed.
SSH Timeout	The SSH timeout value in minutes.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.

Management Security Commands

This section describes commands you use to generate keys and certificates, which you can do in addition to loading them as before.

crypto certificate generate

Use this command to generate self-signed certificate for HTTPS. The generate RSA key for SSL has a length of 1024 bits. The resulting certificate is generated with a common name equal to the lowest IP address of the device and a duration of 365 days.

Format	`crypto certificate generate`
Mode	Global Config

no crypto certificate generate

Use this command to delete the HTTPS certificate files from the device, regardless of whether they are self-signed or downloaded from an outside source.

Format	`no crypto certificate generate`
Mode	Global Config

crypto key generate rsa

Use this command to generate an RSA key pair for SSH. The new key files will overwrite any existing generated or downloaded RSA key files.

Format	`crypto key generate rsa`
Mode	Global Config

no crypto key generate rsa

Use this command to delete the RSA key files from the device.

Format	`no crypto key generate rsa`
Mode	Global Config

crypto key generate dsa

Use this command to generate a DSA key pair for SSH. The new key files will overwrite any existing generated or downloaded DSA key files.

Format	`crypto key generate dsa`
Mode	Global Config

no crypto key generate dsa

Use this command to delete the DSA key files from the device.

Format	`no crypto key generate dsa`
Mode	Global Config

Hypertext Transfer Protocol (HTTP) Commands

This section describes the commands you use to configure HTTP and secure HTTP access to the switch. Access to the switch by using a Web browser is enabled by default. Everything you can view and configure by using the CLI is also available by using the Web.

ip http server

This command enables access to the switch through the Web interface. When access is enabled, the user can login to the switch from the Web interface. When access is disabled, the user cannot login to the switch's Web server. Disabling the Web interface takes effect immediately. All interfaces are affected.

Default	enabled
Format	`ip http server`
Mode	Privileged EXEC

no ip http server

This command disables access to the switch through the Web interface. When access is disabled, the user cannot login to the switch's Web server.

Format	`no ip http server`
Mode	Privileged EXEC

ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

Default	disabled
Format	`ip http secure-server`
Mode	Privileged EXEC

no ip http secure-server

This command is used to disable the secure socket layer for secure HTTP.

Format	`no ip http secure-server`
Mode	Privileged EXEC

ip http java

This command enables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Default	Enabled
Format	`ip http java`
Mode	Privileged EXEC

no ip http java

This command disables the Web Java mode. The Java mode applies to both secure and un-secure Web connections.

Format	`no ip http java`
Mode	Privileged EXEC

ip http session hard-timeout

This command configures the hard timeout for un-secure HTTP sessions in hours. Configuring this value to zero will give an infinite hard-timeout. When this timeout expires, the user will be forced to re-authenticate. This timer begins on initiation of the web session and is unaffected by the activity level of the connection.

Default	24
Format	`ip http session hard-timeout <0-168>`
Mode	Privileged EXEC

no ip http session hard-timeout

This command restores the hard timeout for un-secure HTTP sessions to the default value.

Format	`no ip http session hard-timeout`
Mode	Privileged EXEC

ip http authentication

This command specifies the authentication methods for http server users. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify none as the final method in the command line. For example If none specified as an authentication method after radius, no authentication is used if the radius server is down.

Format	`ip http authentication` *`method1`* `[`*`method2 ...`*`]`
Mode	Global ConfigC

Term	Definition
Local	Uses the local username database for authentication.
Radius	Uses the list of all RADIUS servers for authentication.
Tacacs	Uses the list of all TACACS servers for authentication.
None	Uses no authentication.

no ip http authentication

This command restores the authentication methods to the default.

Format	`no ip http authentication` *`method1`* `[`*`method2 ...`*`]`
Mode	Global Config

ip http session maxsessions

This command limits the number of allowable un-secure HTTP sessions. Zero is the configurable minimum.

Default	16
Format	`ip http session maxsessions <`*`0-16`*`>`
Mode	Privileged EXEC

no ip http session maxsessions

This command restores the number of allowable un-secure HTTP sessions to the default value.

Format	`no ip http session maxsessions`
Mode	Privileged EXEC

ip http session soft-timeout

This command configures the soft timeout for un-secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires the user will be forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch.

Default	5
Format	`ip http session soft-timeout <0-60>`
Mode	Privileged EXEC

no ip http session soft-timeout

This command resets the soft timeout for un-secure HTTP sessions to the default value.

Format	`no ip http session soft-timeout`
Mode	Privileged EXEC

ip http secure-session maxsessions

This command limits the number of secure HTTP sessions. Zero is the configurable minimum.

Default	16
Format	`ip http secure-session maxsessions <0-16>`
Mode	Privileged EXEC

no ip http secure-session maxsessions

This command restores the number of allowable secure HTTP sessions to the default value.

Format	`no ip http secure-session maxsessions`
Mode	Privileged EXEC

ip http secure-session soft-timeout

This command configures the soft timeout for secure HTTP sessions in minutes. Configuring this value to zero will give an infinite soft-timeout. When this timeout expires, you are forced to re-authenticate. This timer begins on initiation of the Web session and is re-started with each access to the switch. The secure-session soft-timeout can not be set to zero (infinite).

Default	5
Format	`ip http secure-session soft-timeout <1-60>`
Mode	Privileged EXEC

no ip http secure-session soft-timeout

This command restores the soft timeout for secure HTTP sessions to the default value.

Format	`no ip http secure-session soft-timeout`
Mode	Privileged EXEC

ip http secure-session hard-timeout

This command configures the hard timeout for secure HTTP sessions in hours. When this timeout expires, the user is forced to re-authenticate. This timer begins on initiation of the Web session and is unaffected by the activity level of the connection. The secure-session hard-timeout can not be set to zero (infinite).

Default	24
Format	`ip http secure-session hard-timeout <1-168>`
Mode	Privileged EXEC

no ip http secure-session hard-timeout

This command resets the hard timeout for secure HTTP sessions to the default value.

Format	`no ip http secure-session hard-timeout`
Mode	Privileged EXEC

ip https authentication

This command specifies the authentication methods for http server users. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. If `none` is specified as an authentication method after `radius`, no authentication is used if the radius server is down.

Format	`ip https authentication` *`method1`* `[`*`method2 ...`*`]`
Mode	Global ConfigC

Term	Definition
Local	Uses the local username database for authentication.
Radius	Uses the list of all RADIUS servers for authentication.
Tacacs	Uses the list of all TACACS servers for authentication.
None	Uses no authentication.

no ip https authentication

This command restores the authentication methods to the default for http server users.

Format	`no ip https authentication` *`method1`* `[`*`method2 ...`*`]`
Mode	Global Config

ip http secure-port

This command is used to set the SSL port where port can be 1-65535 and the default is port 443.

Default	443

Format	`ip http secure-port <portid>`
Mode	Privileged EXEC

no ip http secure-port

This command is used to reset the SSL port to the default value.

Format	`no ip http secure-port`
Mode	Privileged EXEC

ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

Default	SSL3 and TLS1
Format	`ip http secure-protocol [SSL3] [TLS1]`
Mode	Privileged EXEC

show ip http

This command displays the http settings for the switch.

Format	`show ip http`
Mode	Privileged EXEC

Term	Definition
HTTP Mode (Unsecure)	The unsecure HTTP server administrative mode.
Java Mode	The java applet administrative mode which applies to both secure and un-secure web connections.
Maximum Allowable HTTP Sessions	The number of allowable un-secure http sessions.
HTTP Session Hard Timeout	The hard timeout for un-secure http sessions in hours.
HTTP Session Soft Timeout	The soft timeout for un-secure http sessions in minutes.
HTTP Mode (Secure)	The secure HTTP server administrative mode.
Secure Port	The secure HTTP server port number.

Term	Definition
Secure Protocol Level(s)	The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.
Maximum Allowable HTTPS Sessions	The number of allowable secure http sessions.
HTTPS Session Hard Timeout	The hard timeout for secure http sessions in hours.
HTTPS Session Soft Timeout	The soft timeout for secure http sessions in minutes.
Certificate Present	Indicates whether the secure-server certificate files are present on the device.
Certificate Generation in Progress	Indicates whether certificate generation is currently in progress.

Access Commands

Use the commands in this section to close remote connections or to view information about connections to the system.

disconnect

Use the **`disconnect`** command to close HTTP, HTTPS, Telnet or SSH sessions. Use *`all`* to close all active sessions, or use *`<session-id>`* to specify the session ID to close. To view the possible values for *`<session-id>`*, use the **`show loginsession`** command.

Format	`disconnect {<session_id>	all}`
Mode	Privileged EXEC

show loginsession

This command displays current Telnet and serial port connections to the switch.

Format	`show loginsession`
Mode	Privileged EXEC

Term	Definition
ID	Login Session ID.

Term	Definition
User Name	The name the user entered to log on to the system.
Connection From	IP address of the remote client machine or EIA-232 for the serial port connection.
Idle Time	Time this session has been idle.
Session Time	Total time this session has been connected.
Session Type	Shows the type of session, which can be HTTP, HTTPS, telnet, serial, or SSH.

User Account Commands

This section describes the commands you use to add, manage, and delete system users. The 7000 series software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

Note: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

username

Use this command to add a new user to the local user database. The default privilege level is 1. Using the encrypted keyword allows the administrator to transfer local user passwords between devices without having to know the passwords. When the password parameter is used along with encrypted parameter, the password must be exactly 128 hexadecimal characters in length. If the password strength feature is enabled, this command checks for password strength and returns an appropriate error if it fails to meet the password strength criteria. Giving the optional parameter override-complexity-check disables the validation of the password strength.

Format
```
username <name> password <password> [level level] [encrypted]
[overridecomplexity-check]
```

Mode Global Config

Term	Definition
Name	The name of the user, up to 32 characters.

Term	Definition
Password	The password for the users 8-64 characters. This value can be zero if the no passwords min-length command has been executed. The special characters allowed in the password include: ! # $ % & ' ( ) * + , - . / : ; < = > @ [\ ] ^ _ ` { | } ~.
level	Specifies the user level. If not specified, the privilege level is 1. Level 0 can be assigned by a level 15 user to another user to suspend that user’s access. Range 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access.
encrypted	Encrypted password you enter, copied from another device configuration.
override-complexity-check	Disables the validation of the password strength.

no username

This command removes a user account.

Format	`no username <username>`
Mode	Global Config

Note: You cannot delete the “admin” user account.

username nopassword

This command removes the password from a user.

Format	`username <name> nopassword [level level]`
Mode	Global Config

username <*username*> unlock

Use this command to unlock a locked user account. Only a user with read/write access can re-activate a locked user account.

Format	`username <username> unlock`
Mode	Global Config

username snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are **readonly** or **readwrite**. The *<username>* is the login user name for which the specified access mode applies. The default is **readwrite** for the “admin” user and **readonly** for all other users. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Defaults	• admin - readwrite • other - readonly
Format	`username snmpv3 accessmode <username> {readonly	readwrite}`
Mode	Global Config

no username snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified user as **readwrite** for the “admin” user and **readonly** for all other users. The *<username>* value is the user name for which the specified access mode will apply.

Format	`no username snmpv3 accessmode <username>`
Mode	Global Config

username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified user. The valid authentication protocols are **none**, **md5** or **sha**. If you specify **md5** or **sha**, the login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The *<username>* is the user name associated with the authentication protocol. You must enter the *<username>* in the same case you used when you added the user. To see the case of the *<username>*, enter the **show users** command.

Default	no authentication
Format	`username snmpv3 authentication <username> {none	md5	sha}`
Mode	Global Config

no username snmpv3 authentication

This command sets the authentication protocol to be used for the specified user to **none**. The `<username>` is the user name for which the specified authentication protocol is used.

Format	`no username snmpv3 authentication <username>`
Mode	Global Config

username snmpv3 encryption

This command specifies the encryption protocol used for the specified user. The valid encryption protocols are **`des`** or **`none.`**

If you select **`des`**, you can specify the required key on the command line. The encryption key must be 8 to 64 characters long. If you select the **`des`** protocol but do not provide a key, the user is prompted for the key. When you use the **`des`** protocol, the login password is also used as the snmpv3 encryption password, so it must be a minimum of eight characters. If you select **`none`**, you do not need to provide a key.

The `<username>` value is the login user name associated with the specified encryption. You must enter the `<username>` in the same case you used when you added the user. To see the case of the `<username>`, enter the **`show users`** command.

Default	no encryption
Format	`username snmpv3 encryption <username> {none | des[key]}`
Mode	Global Config

no username snmpv3 encryption

This command sets the encryption protocol to **none**. The `<username>` is the login user name for which the specified encryption protocol will be used.

Format	`no username snmpv3 encryption <username>`
Mode	Global Config

show users

This command displays the configured user names and their settings. This command is only available for users with Read/Write privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format	`show users`
Mode	Privileged EXEC

Term	Definition
User Name	The name the user enters to login using the serial port, Telnet or Web.
Access Mode	Shows whether the user is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the “admin” user has Read/Write access and the “guest” has Read Only access. There can only be one Read/Write user and up to five Read Only users.
SNMPv3 Access Mode	The SNMPv3 Access Mode. If the value is set to **`ReadWrite,`** the SNMPv3 user is able to set and retrieve parameters on the system. If the value is set to **`ReadOnly,`** the SNMPv3 user is only able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.
SNMPv3 Authentication	The authentication protocol to be used for the specified login user.
SNMPv3 Encryption	The encryption protocol to be used for the specified login user.

show users accounts

This command displays the local user status with respect to user account lockout and password aging.

Format	`show users accounts`
Mode	Privileged EXEC

Term	Definition
User Name	The local user account’s user name.
Privilege	The user’s privilege level (1-15).
Password aging	The password aging time for the local users.
Lockout Status	Indicates whether the user account is locked out (true or false).

Term	Definition
Password Expiration Date	The current password expiration date in date format.

show users long

This command is used to display the users full name.

Format	`show users long`
Mode	Privileged EXEC

Term	Definition
User Name	The full name of the user.

show users login-history

This command is used to display the users who have logged in previously.

Format	`show users login-history [{user name}]`
Mode	Privileged EXEC

Term	Definition
Login Time	The time at which the user logged in.
Username	The user name used to login.
Protocol	The protocol that the user used to login.
Location	The location of the user.

passwords min-length

Use this command to enforce a minimum password length for local users. The value also applies to the enable password. The valid range is 0-64.

Default	8
Format	`passwords min-length <0-64>`
Mode	Global Config

no passwords min-length

Use this command to set the minimum password length to the default value.

Format	`no passwords min-length`
Mode	Global Config

passwords history

Use this command to set the number of previous passwords that shall be stored for each user account. When a local user changes his or her password, the user will not be able to reuse any password stored in password history. This ensures that users don’t reuse their passwords often. The valid range is 0-10.

Default	0
Format	`passwords history <`*`0-10`*`>`
Mode	Global Config

no passwords history

Use this command to set the password history to the default value.

Format	`no passwords history`
Mode	Global Config

passwords aging

Use this command to implement aging on passwords for local users. When a user’s password expires, the user will be prompted to change it before logging in again. The valid range is 1-365. The default is 0, or no aging.

Default	0
Format	`passwords aging <`*`1-365`*`>`
Mode	Global Config

no passwords aging

Use this command to set the password aging to the default value.

Format	`no passwords aging`
Mode	Global Config

passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. Password lockout does not apply to logins from the serial console. The valid range is 1-5. The default is 0, or no lockout count enforced.

Format	`passwords lock-out <1-5>`
Mode	Global Config
Default	0

no passwords lock-out

Use this command to set the password lock-out count to the default value.

Format	`no passwords lock-out`
Mode	Global Config

passwords strength-check

Use this command to enable the password strength feature. It is used to verify the strength of a password during configuration.

Format	*`passwords strength-check`*
Mode	Global Config
Default	Disable

no passwords strength-check

Use this command to disable the password strength-check.

Format	`no passwords strength-check`
Mode	Global Config

passwords strength minimum uppercase-letters

Use this command to enforce a minimum number of uppercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Format	*`passwords strength minimum uppercase-letters`*
Mode	Global Config
Default	2

no passwords strength minimum uppercase-letters

Use this command to reset the minimum number of uppercase letters to the default value.

Format	*`no passwords strength minimum uppercase-characters`*
Mode	Global Config

passwords strength minimum lowercase-letters

Use this command to enforce a minimum number of lowercase letters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Format	*`passwords strength minimum lowercase-letters`*
Mode	Global Config
Default	2

no passwords strength minimum lowercase-letters

Use this command to reset the minimum number of lowercase letters to the default value.

Format	`no passwords strength minimum lowercase-characters`
Mode	Global Config

passwords strength minimum numeric-characters

Use this command to enforce a minimum number of numeric characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Format	`passwords strength minimum numeric-letters`
Mode	Global Config
Default	2

no passwords strength minimum numeric-characters

Use this command to reset the minimum number of numeric characters to the default value.

Format	`no passwords strength minimum numeric-characters`
Mode	Global Config

passwords strength minimum special-characters

Use this command to enforce a minimum number of special characters that a password should contain. The valid range is 0-16. The default is 2. Minimum of 0 means no restriction on that set of characters.

Format	`passwords strength minimum special-letters`
Mode	Global Config
Default	2

no passwords strength minimum special-letters

Use this command to reset the minimum number of special letters to the default value.

Format	`no passwords strength minimum special-letters`
Mode	Global Config

passwords strength maximum consecutive-characters

Use this command to enforce a maximum number of consecutive characters that a password should contain. An example of consecutive characters is abcd. The valid range is 0-16. If a password has consecutive characters more than the configured limit, it fails to configure. The default is 0. A maximum of 0 means no restriction on that set of characters.

Format	`passwords strength maximum consecutive-characters`
Mode	Global Config
Default	0

no passwords strength maximum consecutive-characters

Use this command to reset the maximum number of consecutive characters to the default value.

Format	`no passwords strength maximum consecutive-characters`
Mode	Global Config

passwords strength maximum repeated-characters

Use this command to enforce a maximum number of repeated characters that a password should contain. An example of repeated characters is aaaa. The valid range is 0-16. If a password has a repetition of characters more than the configured limit, it fails to configure. The default is 0. A maximum of 0 means no restriction on that set of characters.

Format	`passwords strength maximum repeated-characters`
Mode	Global Config
Default	0

no passwords strength maximum repeated-characters

Use this command to reset the maximum number of repeated-characters to the default value.

Format	*`no passwords strength maximum repeated-characters`*
Mode	Global Config

passwords strength minimum character-classes

Use this command to enforce a minimum number of characters classes that a password should contain. Character classes are uppercase letters, lowercase letters, numeric characters and special characters. The valid range is 0-4. The default is 4.

Format	*`passwords strength minimum character-classes`*
Mode	Global Config
Default	4

no passwords strength minimum character-classes

Use this command to reset the minimum number of character classes to the default value.

Format	*`no passwords strength minimum character-classes`*
Mode	Global Config

passwords strength exclude-keyword

Use this command to exclude the specified keyword while configuring the password. The password does not accept the keyword in any form (in between the string, case insensitive and reverse) as a substring. User can configure up to a maximum of 3 keywords.

Format	*`passwords strength exclude-keyword keyword`*
Mode	Global Config

no passwords strength exclude-keyword

Use this command to remove the exclude-keyword.

Format	*no passwords strength exclude-keyword*
Mode	Global Config

show passwords configuration

Use this command to display the configured password management settings.

Format	*show passwords configuration*
Mode	Privileged EXEC

Termd	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password History	Number of passwords to store for reuse prevention.
Password Aging	Length in days that a password is valid.
Lockout Attempts	Number of failed password login attempts before lockout.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when configuring passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when configuring passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when configuring passwords.
Maximum Password Consecutive Characters	Maximum number of consecutive characters required that the password should contain when configuring passwords.
Maximum Password Repeated Characters	Maximum number of repetition of characters that the password should contain when configuring passwords.
Minimum Password Character Classes	Minimum number of character classes (uppercase, lowercase, numeric and special) required when configuring passwords.
Password Exclude-Keywords	The set of keywords to be excluded from the configured password when strength checking is enabled.

show passwords result

Use this command to display the last password set result information.

Format	`show passwords result`
Mode	Privileged EXEC

Termd	Definition
Last User Whose Password Is Set	Shows the name of the user with the most recently set password.
Password Strength Check	Shows whether password strength checking is enabled.
Last Password Set Result	Shows whether the attempt to set a password was successful. If the attempt failed, the reason for the failure is included.

aaa authentication login

This command is used to set authentication at login. The default and optional list names that you create with the `aaa authentication login` command are used with the `login authentication` command. Create a list by entering the `aaa authentication login` *`list-name method`* command for a particular protocol, where *`list-name`* is any character string used to name this list. The *`method`* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The additional methods of authentication are used only if the previous method returns an error, not if it fails.

An example of a method that returns an error is if a RADIUS server is not present, and an example of a method failing is when a RADIUS server cannot authenticate the client. If ‘local’ method is listed first, since local authentication is always available, it only has the fail condition, not error. As such, if ‘local’ method is the first in the list, no other method will be tried.

To ensure that the authentication succeeds even if all methods return an error, specify *`none`* as the final method in the command line. For example if *`none`* is specified as an authentication method after `radius`, no authentication is used if the radius server is down.

where:

Format	`aaa authentication login {default	*list-name*} *method1* [*method2*...]`
Mode	Global Config

Default Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.

list-name Character string used to name the list of authentication methods activated when a user logs in. Up to 12 characters.

method1 [method2…] At least one from the following table:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
tacacs	Uses the list of all TACACS servers for authentication.

➡ **Note:** The local user database is checked. This has the same effect as the following command: `aaa authentication login local`

no aaa authentication login

This command is used to remove authentication at login.

Format	`no aaa authentication login {default	*list-name*}`
Mode	Global Config

aaa authentication enable

This command is used to set authentication when the user access higher privilege level, use the `aaa authentication enable default` command in global configuration mode. The default and optional list names that you create with the `aaa authentication enable` command are used with the `enable authentication` command.

Create a list by entering the `aaa authentication enable` *`list-name method`* command where *`list-name`* is any character string used to name this list. The *`method`* argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example, if *`none`* is specified as an authentication method after `radius`, no authentication is used if the radius server is down. All `aaa authentication enable default` requests sent by the switch to a RADIUS or TACACS server include the username "`$enabx$`.", where *x* is the requested privilege level.

.

Format	`aaa authentication enable {default | ` *`list-name`*`}` *`method1`* `[`*`method2`*`...]`
Mode	Global Config

Default Uses the listed authentication methods that follow this argument as the default list of methods when a user accesses a higher privilege level.

list-name Character string used to name the list of authentication methods activated when a user accesses a higher privilege level. Up to 12 characters.

method1 [method2…] At least one from the following table:

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication. Uses username "$enabx$."where x is the privilege level.
tacacs	Uses the list of all TACACS servers for authentication. Uses username "$enabx$." where x is the privilege level.

no aaa authentication enable

Note: If the default list is not set, only the enable password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

On the console, the enable password is used if it exists. If no password is set, the process will succeed anyway. This has the same effect as the following command:

```
aaa authentication enable default enable none
```

Use this command to remove the authentication method.

Format	`no aaa authentication enable {default	list-name} method1 [method2...]`
Mode	Global Config

aaa authentication dot1x

This command is used to set authentication for dot1x users. The method argument identifies the list of methods that the authentication algorithm tries, in the given sequence. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. To ensure that the authentication succeeds even if all methods return an error, specify `none` as the final method in the command line. For example if `none` is specified as an authentication method after radius, no authentication is used if the radius server is down.

Format	`aaa authentication dot1x default method1 [method2...]`
Mode	Global Config

method1 [method2…] At least one from the following table:

Keyword	Description
local	Uses the local username database for authentication.
none	Uses no authentication.
radius	Uses the list of all RADIUS servers for authentication.
ias	Uses the internal authentication server users database for authentication.

no aaa authentication dot1x

Use this command to remove the authentication at login.

Format	`no aaa authentication dot1x default`
Mode	Global Config

aaa ias-user username

The Internal Authentication Server (IAS) database is a dedicated internal database used for local authentication of users for network access through the IEEE 802.1X feature. Use this command to add the specified user to the internal user database. This command also changes the mode to AAA User Config mode.

Format	`aaa ias-username <user>`
Mode	Global Config

no aaa ias-user username

Use this command to remove an ias user.

Format	`no aaa ias-username <user>`
Mode	Global Config

password (AAA IAS User Configuration)

Use this command to specify a password for a user in the IAS database.

Format	`password <password> [encrypted]`
Mode	AAA IAS User Config

Parameter	Definition
password	Password for this level. Range: 8-64 characters.
encrypted	Encrypted password to be entered, copied from another switch configuration.

no password(AAA IAS User Configuration)

Use this command to remove a password for a user in the IAS database.

Format	`no password`
Mode	AAA IAS User Config

clear aaa ias-users

Use this command to remove all users from the IAS database.

Format	`clear aaa ias-users`
Mode	Privileged EXEC

show aaa ias-users

Use this command to display configured IAS users and their attributes. Passwords configured are not shown in the show command output.

Format	`show aaa ias-users`
Mode	Privileged EXEC

SNMP Commands

This section describes the commands you use to configure Simple Network Management Protocol (SNMP) on the switch. You can configure the switch to act as an SNMP agent so that it can communicate with SNMP managers on your network.

snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network. The range for *`<name>`*, *`<loc>`* and *`<con>`* is from 1 to 31 alphanumeric characters.

Default	none

Format `snmp-server {sysname <name> | location <loc> | contact <con>}`

Mode Global Config

snmp-server community

This command adds (and names) a new SNMP community. A community `<name>` is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of `<name>` can be up to 16 case-sensitive characters.

Note: Community names in the SNMP Community Table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default
- Public and private, which you can rename.
- Default values for the remaining four community names are blank.

Format `snmp-server community <name>`

Mode Global Config

no snmp-server community

This command removes this community name from the table. The `<name>` is the community name to be deleted.

Format `no snmp-server community <name>`

Mode Global Config

snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default 0.0.0.0

Format	`snmp-server community ipaddr <ipaddr> <name>`
Mode	Global Config

no snmp-server community ipaddr

This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format	`no snmp-server community ipaddr <name>`
Mode	Global Config

snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default	0.0.0.0
Format	**`snmp-server community ipmask`** `<ipmask> <name>`
Mode	Global Config

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

Format	`no snmp-server community ipmask <name>`
Mode	Global Config

snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default	• private and public communities - enabled • other four - disabled
Format	`snmp-server community mode <`*`name`*`>`
Mode	Global Config

no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Format	`no snmp-server community mode <`*`name`*`>`
Mode	Global Config

snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format	`snmp-server community ro <`*`name`*`>`
Mode	Global Config

snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format	`snmp-server community rw <`*`name`*`>`
Mode	Global Config

snmp-server enable traps violation

This command enables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

Note: For other port security commands, see “Protected Ports Commands” on page 3-53.

Default	disabled
Format	`snmp-server enable traps violation`
Mode	Interface Config

no snmp-server enable traps violation

This command disables the sending of new violation traps.

Format	`no snmp-server enable traps violation`
Mode	Interface Config

snmp-server enable traps

This command enables the Authentication Flag.

Default	enabled
Format	`snmp-server enable traps`
Mode	Global Config

no snmp-server enable traps

This command disables the Authentication Flag.

Format	`no snmp-server enable traps`
Mode	Global Config

snmp-server enable traps linkmode

Note: This command may not be available on all platforms.

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled. See “snmp trap link-status” on page 7-55

Default	enabled
Format	`snmp-server enable traps linkmode`
Mode	Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format	`no snmp-server enable traps linkmode`
Mode	Global Config

snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or Telnet) and there is an existing terminal interface session.

Default	enabled
Format	`snmp-server enable traps multiusers`
Mode	Global Config

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format	`no snmp-server enable traps multiusers`
Mode	Global Config

snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default	enabled
Format	`snmp-server enable traps stpmode`
Mode	Global Config

no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format	`no snmp-server enable traps stpmode`
Mode	Global Config

snmptrap

This command adds an SNMP trap receiver. The maximum length of *<name>* is 16 case-sensitive alphanumeric characters. The *<snmpversion>* is the version of SNMP. The version parameter options are snmpv1 or snmpv2. The SNMP trap address can be set using both an IPv4 address format as well as an IPv6 global address format.

The following shows an example of the CLI command.

```
(Netgear Switch)# snmptrap mytrap ip6addr 3099::2
```

Note: The <*name*> parameter does not need to be unique, however; the <*name*> and <*ipaddr* | *hostname*> pair must be unique. Multiple entries can exist with the same <*name*>, as long as they are associated with a different <*ipaddr* | *hostname*>. The reverse scenario is also acceptable. The <*name*> is the community name used when sending the trap to the receiver, but the <*name*> is not directly associated with the SNMP Community Table, See “snmp-server community” on page39.”

Default	snmpv2
Format	`snmptrap` *`<name> {ipaddr <ipaddr|hostname>	ip6addr <ip6addr|hostname>} [snmpversion <snmpversion>]`*
Mode	Global Config

no snmptrap

This command deletes trap receivers for a community.

Format	`no snmptrap <name> {ipaddr <ipaddr|hostname>	ip6addr <ip6addr|hostname>}`
Mode	Global Config

snmptrap snmpversion

This command modifies the SNMP version of a trap. The maximum length of `<name>` is 16 case-sensitive alphanumeric characters. The `<snmpversion>` parameter options are snmpv1 or snmpv2.

> **Note:** This command does not support a “no” form.

Default	snmpv2
Format	`snmptrap snmpversion <name> {<ipaddr	hostname> |<ip6addr|hostname>} {snmpv1|snmpv2}`
Mode	Global Config

snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

> **Note:** IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format	`snmptrap ipaddr <name> <ipaddrold> <ipaddrnew	hostnamenew>`
Mode	Global Config

snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format	`snmptrap mode <name> { <ipaddr | hostname> |<ip6addr |hostname>}`
Mode	Global Config

no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are unable to receive traps.

Format	`no snmptrap mode <name> { <ipaddr | hostname> |<ip6addr |hostname>}`
Mode	Global Config

snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See "snmp-server enable traps linkmode" on page 7-52

Format	`snmp trap link-status`
Mode	Interface Config

no snmp trap link-status

This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled.

Format	`no snmp trap link-status`
Mode	Interface Config

snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See "snmp-server enable traps linkmode" on page 7-52

Format	`snmp trap link-status all`
Mode	Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See "snmp-server enable traps linkmode" on page 7-52

Format	`no snmp trap link-status all`
Mode	Global Config

show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP Versions 1, 2 or 3. For more information about the SNMP specification, see the SNMP RFCs. The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format	`show snmpcommunity`
Mode	Privileged EXEC

Term	Definition
SNMP Community Name	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
Client IP Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP address. Note: If the Subnet Mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0.
Client IP Mask	A mask to be ANDed with the requesting entity's IP address before comparison with IP address. If the result matches with IP address then the address is an authenticated IP address. For example, if the IP address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
Access Mode	The access level for this community string.
Status	The status of this community access entry.

show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format	`show snmptrap`
Mode	Privileged EXEC

Term	Definition
SNMP Trap Name	The community string of the SNMP trap packet sent to the trap manager. The string is case sensitive and can be up to 16 alphanumeric characters.
IP Address	The IPv4 address to receive SNMP traps from this device.
IPv6 Address	The IPv6 address to receive SNMP traps from this device.
SNMP Version	SNMPv2
Status	The receiver's status (enabled or disabled).

The following shows an example of the CLI command.

```
(Netgear Switch)#show snmptrap

 Community Name   IpAddress     IPv6 Address     Snmp Version    Mode
   Mytrap        0.0.0.0       2001::1        SNMPv2        Enable show trapflags
```

show trapflags

This command displays trap conditions. The command’s display shows all the enabled OSPFv2 and OSPFv3 trapflags. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the SNMP agent on the switch sends the trap to all enabled trap receivers. You do not have to reset the switch to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format	`show trapflags`
Mode	Privileged EXEC

Term	Definition
Authentication Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).
Spanning Tree Flag	Can be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps are sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps are sent.
DVMRP Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether DVMRP traps are sent.
OSPFv2 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPF trap flags are not enabled, then the command displays *`disabled`*. Otherwise, the command shows all the enabled OSPF traps’ information.
OSPFv3 Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps are sent. If any of the OSPFv3 trap flags are not enabled, then the command displays *`disabled`*. Otherwise, the command shows all the enabled OSPFv3 traps’ information.
PIM Traps	Can be enabled or disabled. The factory default is disabled. Indicates whether PIM traps are sent.

RADIUS Commands

This section describes the commands you use to configure the switch to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

authorization network radius

Use this command to enable the switch to accept VLAN assignment by the radius server.

Default	disable
Format	`authorization network radius`
Mode	Global Config

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the radius server.

Format	`no authorization network radius`
Mode	Global Config

radius accounting mode

This command is used to enable the RADIUS accounting function.

Default	disabled
Format	`radius accounting mode`
Mode	Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format	`no radius accounting mode`
Mode	Global Config

radius server attribute

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format	`radius server attribute <4> [<`*`ipaddr`*`>]`
Mode	Global Config

Term	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

no radius server attribute

The no version of this command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format	`no radius server attribute <4> [<`*`ipaddr`*`>]`
Mode	Global Config

The following shows an example of the command.

```
(Switch) (Config) #radius server attribute 4  192.168.37.60
(Switch) (Config) #radius server attribute 4
```

radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the 'Default_RADIUS_Auth_Server' and 'Default_RADIUS_Acct_Server' as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers. The RADIUS client allows the configuration of a maximum 32 authenticating and accounting servers.

If you use the `<auth>` parameter, the command configures the IP address or hostname to use to connect to a RADIUS authentication server. You can configure up to 3 servers per RADIUS client. If the maximum number of configured servers is reached, the command fails until you remove one of the servers by issuing the "no" form of the command. If you use the optional `<port>` parameter, the command configures the UDP port number to use when connecting to the configured RADIUS server. The `<port>` number range is 1 - 65535, with 1812 being the default value.

Note: To re-configure a RADIUS authentication server to use the default UDP <*port*>, set the <*port*> parameter to 1812.

If you use the `<acct>` token, the command configures the IP address or hostname to use for the RADIUS accounting server. You can only configure one accounting server. If an accounting server is currently configured, use the "no" form of the command to remove it from the configuration. The IP address or hostname you specify must match that of a previously configured accounting server. If you use the optional `<port>` parameter, the command configures the UDP port to use when connecting to the RADIUS accounting server. If a `<port>` is already configured for the accounting server, the new `<port>` replaces the previously configured `<port>`. The `<port>` must be a value in the range 0 - 65535, with 1813 being the default.

Note: To re-configure a RADIUS accounting server to use the default UDP <*port*>, set the <*port*> parameter to 1813.

Format

```
radius server host {auth | acct} {<ipaddr|dnsname>} [name
<servername>] [port <0-65535>][server-type]
```

Mode Global Config

Field	Description
ipaddr	The IP address of the server.

Field	Description
dnsname	The DNS name of the server.
0-65535	The port number to use to connect to the specified RADIUS server.
servername	The alias name to identify the server.

no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The *<ipaddr|dnsname>* parameter must match the IP address or dns name of the previously configured RADIUS authentication / accounting server.

Format	no radius server host *{auth | acct}* {<*ipaddr*|*dnsname*>}
Mode	Global Config

The following shows an example of the command.

```
(Switch) (Config) #radius server host acct 192.168.37.60
(Switch) (Config) #radius server host acct 192.168.37.60 port 1813
(Switch) (Config) #radius server host auth 192.168.37.60 name 
Network1_RADIUS_Auth_Server port 1813

(Switch) (Config) #radius server host acct 192.168.37.60 name 
Network2_RADIUS_Auth_Server
(Switch) (Config) #no radius server host acct 192.168.37.60
```

radius server key

This command configures the key to be used in RADIUS client communication with the specified server. Depending on whether the 'auth' or 'acct' token is used, the shared secret is configured for the RADIUS authentication or RADIUS accounting server. The IP address or hostname provided must match a previously configured server. When this command is executed, the secret is prompted.

Text-based configuration supports Radius server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

➡	**Note:** The secret must be an alphanumeric value not exceeding 16 characters.

Format	`radius server key {`*`auth`*`	`*`acct`*`} {<`*`ipaddr`*`|`*`dnsname`*`>} encrypted <`*`password`*`>`
Mode	Global Config

Field	Description
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
password	The password in encrypted format.

The following shows an example of the CLI command.

```
radius server key acct 10.240.4.10 encrypted <encrypt-string>
```

radius server msgauth

This command enables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	`radius server msgauth <`*`ipaddr`*`|`*`dnsname`*`>`
Mode	Global Config

Field	Description
ip addr	The IP address of the server.
dnsname	The DNS name of the server.

no radius server msgauth

The no version of this command disables the message authenticator attribute to be used for the specified RADIUS Authenticating server.

Format	`no radius server msgauth <ipaddr|dnsname>`
Mode	Global Config

radius server primary

This command specifies a configured server that should be the primary server in the group of servers which have the same server name. Multiple primary servers can be configured for each number of servers that have the same name. When the RADIUS client has to perform transactions with an authenticating RADIUS server of specified name, the client uses the primary server that has the specified server name by default. If the RADIUS client fails to communicate with the primary server for any reason, the client uses the backup servers configured with the same server name. These backup servers are identified as the ‘Secondary’ type.

Format	`radius server primary {<ipaddr|dnsname>}`
Mode	Global Config

Field	Description
ip addr	The IP address of the RADIUS Authenticating server.
dnsname	The DNS name of the server.

radius server retransmit

This command configures the global parameter for the RADIUS client that specifies the number of transmissions of the messages to be made before attempting the fall back server upon unsuccessful communication with the current RADIUS authenticating server. When the maximum number of retries are exhausted for the RADIUS accounting server and no response is received, the client does not communicate with any other server.

Default	4
Format	`radius server retransmit <retries>`
Mode	Global Config

Field	Description
retries	The maximum number of transmission attempts in the range of 1 to 15.

no radius server retransmit

The no version of this command sets the value of this global parameter to the default value.

Format	`no radius server retransmit`
Mode	Global Config

radius server timeout

This command configures the global parameter for the RADIUS client that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default	5
Format	`radius server timeout <`*`seconds`*`>`
Mode	Global Config

Field	Description
retries	Maximum number of transmission attempts in the range <1-30>.

no radius server timeout

The no version of this command sets the timeout global parameter to the default value.

Format	`no radius server timeout`
Mode	Global Config

show radius

This command displays the values configured for the global parameters of the RADIUS client.

Format	`show radius`
Mode	Privileged EXEC

Term	Definition
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Time Duration	The configured timeout value, in seconds, for request re-transmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.

The following shows example CLI display output for the command.

```
(Switch)#show radius

        Number of Configured Authentication Servers............. 32
        Number of Configured Accounting Servers................. 32
        Number of Named Authentication Server Groups............ 15
        Number of Named Accounting Server Groups................ 3
        Number of Retransmits................................... 4
        Time Duration........................................... 10
        RADIUS Accounting Mode.................................. Disable
        RADIUS Attribute 4 Mode................................. Enable
        RADIUS Attribute 4 Value ............................... 192.168.37.60
```

show radius servers

This command displays the summary and details of RADIUS authenticating servers configured for the RADIUS client.

Format	`show radius servers [ { <ipaddr | dnsname> | name [<servername> ] } ]`
Mode	Privileged EXEC

Field	Description
ipaddr	The IP address of the authenticating server.
dnsname	The DNS name of the authenticating server.
servername	The alias name to identify the server.
Current	The '*' symbol preceeding the server host address specifies that the server is currently active.
Host Address	The IP address of the host.
Server Name	The name of the authenticating server.
Port	The port used for communication with the authenticating server.
Type	Specifies whether this server is a primary or secondary type.
Current Host Address	The IP address of the currently active authenticating server.
Secret Configured	Yes or No Boolean value that indicates whether this server is configured with a secret.
Number of Retransmits	The configured value of the maximum number of times a request packet is retransmitted.
Message Authenticator	A global parameter to indicate whether the Message Authenticator attribute is enabled or disabled.
Time Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in NAS-IP-Address attribute used in RADIUS requests.

The following shows example CLI display output for the command.

```
(Switch) #show radius servers

Cur  Host Address            Server Name                      Port  Type
```

```
rent
---- ------------------------ --------------------------------- ----- ----------
    *   192.168.37.200           Network1_RADIUS_Server           1813  Primary
     192.168.37.201           Network2_RADIUS_Server            1813  Secondary
     192.168.37.202           Network3_RADIUS_Server            1813  Primary
     192.168.37.203           Network4_RADIUS_Server            1813  Secondary

(Switch) #show radius servers name

Current Host Address     Server Name                       Type
------------------------ -------------------------------- ----------
192.168.37.200           Network1_RADIUS_Server            Secondary
192.168.37.201           Network2_RADIUS_Server            Primary
192.168.37.202           Network3_RADIUS_Server            Secondary
192.168.37.203           Network4_RADIUS_Server            Primary

(Switch) #show radius servers name Default_RADIUS_Server

Server Name............................ Default_RADIUS_Server
Host Address........................... 192.168.37.58
Secret Configured...................... No
Message Authenticator ................. Enable
Number of Retransmits.................. 4
Time Duration.......................... 10
RADIUS Accounting Mode................. Disable
RADIUS Attribute 4 Mode................ Enable
RADIUS Attribute 4 Value .............. 192.168.37.60

(Switch) #show radius servers 192.168.37.58

Server Name............................ Default_RADIUS_Server
Host Address........................... 192.168.37.58
Secret Configured...................... No
Message Authenticator ................. Enable
Number of Retransmits.................. 4
Time Duration.......................... 10
RADIUS Accounting Mode................. Disable
RADIUS Attribute 4 Mode................ Enable
RADIUS Attribute 4 Value .............. 192.168.37.60
```

show radius accounting

This command displays a summary of configured RADIUS accounting servers.

Format `show radius accounting name [<servername>]`

Mode Privileged EXEC

Field	Description
servername	An alias name to identify the server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Term	Definition
Host Address	The IP address of the host.
Server Name	The name of the accounting server.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.

The following shows example CLI display output for the command.

```
(Switch) #show radius accounting name

Host Address            Server Name                       Port     Secret
                                                                   Configured
----------------------- --------------------------------- -------- -----------
192.168.37.200          Network1_RADIUS_Server            1813     Yes
192.168.37.201          Network2_RADIUS_Server            1813     No
192.168.37.202          Network3_RADIUS_Server            1813     Yes
192.168.37.203          Network4_RADIUS_Server            1813     No


 (Switch) #show radius accounting name Default_RADIUS_Server

Server Name............................ Default_RADIUS_Server
Host Address........................... 192.168.37.200
RADIUS Accounting Mode................. Disable
Port .................................. 1813
Secret Configured ..................... Yes
```

show radius accounting statistics

This command displays a summary of statistics for the configured RADIUS accounting servers.

Format	`show radius accounting statistics {<ipaddr|dnsname>	name <servername>}`
Mode	Privileged EXEC

Term	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.
servername	The alias name to identify the server.
RADIUS Accounting Server Name	The name of the accounting server.
Server Host Address	The IP address of the host.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Retransmission	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

The following shows example CLI display output for the command.

```
(Switch) #show radius accounting statistics 192.168.37.200

RADIUS Accounting Server Name................. Default_RADIUS_Server
Host Address.................................. 192.168.37.200
Round Trip Time............................... 0.00
Requests...................................... 0
Retransmissions............................... 0
Responses..................................... 0
Malformed Responses........................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0

(Switch) #show radius accounting statistics name Default_RADIUS_Server

RADIUS Accounting Server Name................. Default_RADIUS_Server
Host Address.................................. 192.168.37.200
Round Trip Time............................... 0.00
Requests...................................... 0
Retransmissions............................... 0
Responses..................................... 0
Malformed Responses........................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
Timeouts...................................... 0
Unknown Types................................. 0
Packets Dropped............................... 0
```

show radius statistics

This command displays the summary statistics of configured RADIUS Authenticating servers.

Format `show radius statistics {<ipaddr|dnsname> | name <servername>}`

Mode Privileged EXEC

Term	Definition
ipaddr	The IP address of the server.
dnsname	The DNS name of the server.

Term	Definition
servername	The alias name to identify the server.
RADIUS Server Name	The name of the authenticating server.
Server Host Address	The IP address of the host.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

The following shows example CLI display output for the command.

```
(Switch) #show radius statistics 192.168.37.200

RADIUS Server Name............................ Default_RADIUS_Server
Server Host Address........................... 192.168.37.200
Access Requests............................... 0.00
Access Retransmissions........................ 0
Access Accepts................................ 0
Access Rejects................................ 0
Access Challenges............................. 0
Malformed Access Responses.................... 0
Bad Authenticators............................ 0
Pending Requests.............................. 0
```

```
Timeouts..................................... 0
Unknown Types................................ 0
Packets Dropped.............................. 0

(Switch) #show radius statistics name Default_RADIUS_Server

RADIUS Server Name........................... Default_RADIUS_Server
Server Host Address.......................... 192.168.37.200
Access Requests.............................. 0.00
Access Retransmissions....................... 0
Access Accepts............................... 0
Access Rejects............................... 0
Access Challenges............................ 0
Malformed Access Responses................... 0
Bad Authenticators........................... 0
Pending Requests............................. 0
Timeouts..................................... 0
Unknown Types................................ 0
Packets Dropped.............................. 0
```

TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

tacacs-server host

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *<ip-address|hostname>* parameter is the IP address or hostname of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Format	tacacs-server host *<ip-address|hostname>*
Mode	Global Config

no tacacs-server host

Use the **`no tacacs-server host`** command to delete the specified hostname or IP address. The *`<ip-address|hostname>`* parameter is the IP address of the TACACS+ server.

Format	`no tacacs-server host <ip-address|hostname>`
Mode	Global Config

tacacs-server key

Use the **`tacacs-server key`** command to set the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *`<key-string>`* parameter has a range of 0 - 128 characters and specifies the authentication and encryption key for all TACACS communications between the switch and the TACACS+ server. This key must match the key used on the TACACS+ daemon.

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	`tacacs-server key [<key-string>	encrypted <key-string>]`
Mode	Global Config

no tacacs-server key

Use the **`no tacacs-server key`** command to disable the authentication and encryption key for all TACACS+ communications between the switch and the TACACS+ daemon. The *`<key-string>`* parameter has a range of 0 - 128 characters This key must match the key used on the TACACS+ daemon.

Format	`no tacacs-server key <key-string>`
Mode	Global Config

tacacs-server timeout

Use the **`tacacs-server timeout`** command to set the timeout value for communication with the TACACS+ servers. The *`<timeout>`* parameter has a range of 1-30 and is the timeout value in seconds.

Default	5
Format	`tacacs-server timeout <timeout>`
Mode	Global Config

no tacacs-server timeout

Use the **`no tacacs-server timeout`** command to restore the default timeout value for all TACACS servers.

Format	`no tacacs-server timeout`
Mode	Global Config

key

Use the **`key`** command in TACACS Configuration mode to specify the authentication and encryption key for all TACACS communications between the device and the TACACS server. This key must match the key used on the TACACS daemon. The *`<key-string>`* parameter specifies the key name. For an empty string use " ". (Range: 0 - 128 characters).

Text-based configuration supports TACACS server's secrets in encrypted and non-encrypted format. When you save the configuration, these secret keys are stored in encrypted format only. If you want to enter the key in encrypted format, enter the key along with the encrypted keyword. In the show running config command's display, these secret keys are displayed in encrypted format. You cannot show these keys in plain text format.

Format	`key [<key-string> | encrypted <key-string>]`
Mode	TACACS Config

port

Use the **`port`** command in TACACS Configuration mode to specify a server port number. The server *`<port-number>`* range is 0 - 65535.

Default	49
Format	`port` *`<port-number>`*
Mode	TACACS Config

priority

Use the **`priority`** command in TACACS Configuration mode to specify the order in which servers are used, where 0 (zero) is the highest priority. The *`<priority>`* parameter specifies the priority for servers. The highest priority is 0 (zero), and the range is 0 - 65535.

Default	0
Format	`priority` *`<priority>`*
Mode	TACACS Config

timeout

Use the **`timeout`** command in TACACS Configuration mode to specify the timeout value in seconds. If no timeout value is specified, the global value is used. The *`<timeout>`* parameter has a range of 1-30 and is the timeout value in seconds.

Format	`timeout` *`<timeout>`*
Mode	TACACS Config

show tacacs

Use the **`show tacacs`** command to display the configuration and statistics of a TACACS+ server.

Format	`show tacacs` *`[<ip-address|hostname>]`*
Mode	Privileged EXEC

Term	Definition
Host Address	The IP address or hostname of the configured TACACS+ server.
Port	The configured TACACS+ server port number.
TimeOut	The timeout in seconds for establishing a TCP connection.
Priority	The preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.

Configuration Scripting Commands

Configuration Scripting allows you to generate text-formatted script files representing the current configuration of a system. You can upload these configuration script files to a PC or UNIX system and edit them. Then, you can download the edited files to the system and apply the new configuration. You can apply configuration scripts to one or more switches with no or minor modifications.

Use the `show running-config` command (see "show running-config" on page 6-15) to capture the running configuration into a script. Use the `copy` command (see "copy" on page 6-31) to transfer the configuration script to or from the switch.

You should use scripts on systems with default configuration; however, you are not prevented from applying scripts on systems with non-default configurations.

Scripts must conform to the following rules:

- Script files are not distributed across the stack, and only live in the unit that is the master unit at the time of the file download.
- The file extension must be ".scr".
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 2048 KB.
- The maximum number of configuration file command lines is 2000.

You can type single-line annotations at the command prompt to use when you write test or configuration scripts to improve script readability. The exclamation point (!) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line, and all input following this character is ignored. Any command line that begins with the "!" character is recognized as a comment line and ignored by the parser.

The following lines show an example of a script:

```
! Script file for displaying management access
```

```
show telnet !Displays the information about remote connections

! Display information about direct connections

show serial

! End of the script file!
```

Note: To specify a blank password for a user in the configuration script, you must specify it as a space within quotes. For example, to change the password for user `jane` from a blank password to `hello`, the script entry is as follows:

```
users passwd jane
" "
hello
hello
```

script apply

This command applies the commands in the script to the switch. The `<scriptname>` parameter is the name of the script to apply.

Format	`script apply <scriptname>`
Mode	Privileged EXEC

script delete

This command deletes a specified script where the `<scriptname>` parameter is the name of the script to delete. The `<all>` option deletes all the scripts present on the switch.

Format	`script delete {<scriptname> | all}`
Mode	Privileged EXEC

script list

This command lists all scripts present on the switch as well as the remaining available space.

Format	`script list`
Mode	Global Config

Term	Definition
Configuration Script	Name of the script.
Size	Privileged EXEC

script show

This command displays the contents of a script file, which is named `<scriptname>`.

Format	`script show <scriptname>`
Mode	Privileged EXEC

Term	Definition
Output Format	**`line`** `<number>: <line contents>`

script validate

This command validates a script file by parsing each line in the script file where `<scriptname>` is the name of the script to validate.The validate option is intended to be used as a tool for script development. Validation identifies potential problems. It might not identify all problems with a given script on any given device.

Format	`script validate <scriptname>`
Mode	Privileged EXEC

Pre-login Banner and System Prompt Commands

This section describes the commands you use to configure the pre-login banner and the system prompt. The pre-login banner is the text that displays before you login at the **`User:`** prompt.

copy (pre-login banner)

The **copy** command includes the option to upload or download the CLI Banner to or from the switch. You can specify local URLs by using TFTP, Xmodem, Ymodem, or Zmodem.

> **Note:** <*ip6address*> is also a valid parameter for routing packages that support IPv6.

Default	none

Format	`copy <Code Sample Variable><tftp://<ipaddr>/<filepath>/<filename>><Code Sample Variable> nvram:clibanner`
	`copy nvram:clibanner <Code Sample Variable><tftp://<ipaddr>/<filepath>/<filename>><Code Sample Variable>`

Mode	Privileged EXEC

set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format	`set prompt <`*`prompt_string`*`>`
Mode	Privileged EXEC

Switch Database Management (SDM) Templates

You can use SDM templates to configure system resources in the switch and optimize support for specific features depending on how the switch is used in the network. You can select a template to provide the maximum system usage for a specific function. For example, you could use a routing template to optimize resources for IPv4 routing if the network environment does not use IPv6 routing.

Note:

- If you configure an SDM template, you must reload the switch for the configuration to take effect.

- If you try to configure IPv6 routing without first selecting the dual IPv4-IPv6 routing template, a warning message appears.

sdm prefer

This command specifies the SDM template to use on the switch.

Default	ipv4-routing for IPv4 only builds, dual-ipv4-ipv6 for IPv6 builds
Format	`sdm prefer {ipv4-routing {default | data-center} | dual-ipv4-and-ipv6 {default}}`
Mode	Global Config

Parameter	Description
ipv4-routing	Supports IPv4 routing only. `-data-center`: Support more ECMP next hops in IPv4 routes. `-default`: The routing template maximizes system resources for unicast routing, typically required for a router in the center of a network.
dual-ipv4-and-ipv6	Supports both IPv4 and IPv6 routing. This option is visible only when the switch supports IPv6 and IPv4 routing. `-default`: Balance IPv4 and IPv6 Layer 2 and Layer 3 functionality.

no sdm prefer

This command returns to the default template.

Format	`no sdm prefer`
Mode	Global Config

show sdm prefer

This command displays SDM template information.

Format	`show sdm prefer`
Mode	User EXEC

To display the resource numbers supported by the active template, use the `show sdm prefer` privileged EXEC command with no parameters.

Example:

```
(Switch) #show sdm prefer
Current Template: Routing

Active Template: dual-ipv4-ipv6 default
The selected template optimizes the resources in the switch to support maximum
IPv4 routes.
No of IPv4 routes 6k
No of IPV6 routes 0k
```

Chapter 8
Log Messages

This chapter lists common log messages, along with information regarding the cause of each message. There is no specific action that can be taken per message. When there is a problem being diagnosed, a set of these messages in the event log, along with an understanding of the system configuration and details of the problem will assist NETGEAR, Inc. in determining the root cause of such a problem.

➡	**Note:** This chapter is not a complete list of all syslog messages.

The Log Messages chapter includes the following sections:

Core

Table 8-1: BSP Log Messages

Component	**Message**	**Cause**
BSP	Event(0xaaaaaaaa)	Switch has restarted.
BSP	Starting code...	BSP initialization complete, starting 7000 series application.

Table 8-2: NIM Log Messages

Component	**Message**	**Cause**
NIM	NIM: L7_ATTACH out of order for intIfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	There is no mapping between the USP and Interface number
NIM	NIM: L7_DETACH out of order for intIfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: L7_DELETE out of order for intIfNum(x) unit x slot x port x	Interface creation out of order
NIM	NIM: event(x),intf(x),component(x), in wrong phase	An event was issued to NIM during the wrong configuration phase (probably Phase 1, 2, or WMU)
NIM	NIM: Failed to notify users of interface change	Event was not propagated to the system
NIM	NIM: failed to send message to NIM message Queue.	NIM message queue full or non-existent
NIM	NIM: Failed to notify the components of L7_CREATE event	Interface not created
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	A component issued an interface event during the wrong initialization phase
NIM	NIM: incorrect phase for operation	An API call was made during the wrong initialization phase
NIM	NIM: Component(x) failed on event(x) for intIfNum(x)	A component responded with a fail indication for an interface event
NIM	NIM: Timeout event(x), intIfNum(x) remainingMask = “xxxx”	A component did not respond before the NIM timeout occurred

Table 8-3: System Log Messages

Component	Message	Cause
SYSTEM	Configuration file Switch CLI.cfg size is 0 (zero) bytes	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	The configuration file could not be read. This message may occur on a system for which no configuration has ever been saved or for which configuration has been erased.
SYSTEM	Building defaults for file <file name> version <version num>	Configuration did not exist or could not be read for the specified feature or file. Default configuration values will be used. The file name and version are indicated.
SYSTEM	File <filename>: same version (version num) but the sizes (<version size>-><expected version size) differ	The configuration file which was loaded was of a different size than expected for the version number. This message indicates the configuration file needed to be migrated to the version number appropriate for the code image. This message may appear after upgrading the code image to a more current release.
SYSTEM	Migrating config file <filename> from version <version num> to <version num>	The configuration file identified was migrated from a previous version number. Both the old and new version number are specified. This message may appear after upgrading the code image to a more current release.
SYSTEM	Building Defaults	Configuration did not exist or could not be read for the specified feature. Default configuration values will be used.
SYSTEM	sysapiCfgFileGet failed size = <expected size of file> version = <expected version>	Configuration did not exist or could not be read for the specified feature. This message is usually followed by a message indicating that default configuration values will be used.

Utilities

Table 8-4: Trap Mgr Log Message

Component	Message	Cause
Trap Mgr	Link Up/Down: unit/slot/port	An interface changed link state.

Table 8-5: DHCP Filtering Log Messages

Component	Message	Cause
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	Unable to create semaphore used for dhcp filtering configuration structure .
DHCP Filtering	Failed to register with nv Store.	Unable to register save and restore functions for configuration save
DHCP Filtering	Failed to register with NIM	Unable to register with NIM for interface callback functions
DHCP Filtering	Error on call to sysapiCfgFileWrite file	Error on trying to save configuration .

Table 8-6: NVStore Log Messages

Component	Message	Cause
NVStore	Building defaults for file XXX	A component’s configuration file does not exist or the file’s checksum is incorrect so the component’s default configuration file is built.
NVStore	Error on call to osapiFsWrite routine on file XXX	Either the file cannot be opened or the OS’s file I/O returned an error trying to write to the file.
NVStore	File XXX corrupted from file system. Checksum mismatch.	The calculated checksum of a component’s configuration file in the file system did not match the checksum of the file in memory.
NVStore	Migrating config file XXX from version Y to Z	A configuration file version mismatch was detected so a configuration file migration has started.

Table 8-7: RADIUS Log Messages

Component	Message	Cause
RADIUS	RADIUS: Invalid data length - xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to send the request	A problem communicating with the RADIUS server.
RADIUS	RADIUS: Failed to send all of the request	A problem communicating with the RADIUS server during transmit.
RADIUS	RADIUS: Could not get the Task Sync semaphore!	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS Client attempted to build a response larger than resources allow.
RADIUS	RADIUS: Could not allocate accounting requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Could not allocate requestInfo	Resource issue with RADIUS Client service.
RADIUS	RADIUS: osapiSocketRecvFrom returned error	Error while attempting to read data from the RADIUS server.
RADIUS	RADIUS: Accounting-Response failed to validate, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: User (xxx) needs to respond for challenge	An unexpected challenge was received for a configured user.
RADIUS	RADIUS: Could not allocate a buffer for the packet	Resource issue with RADIUS Client service.
RADIUS	RADIUS: Access-Challenge failed to validate, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Failed to validate Message-Authenticator, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Access-Accpet failed to validate, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Invalid packet length – xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Response is missing Message-Authenticator, id=xxx	The RADIUS Client received an invalid message from the server.
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS Client received a server response from an unconfigured server.

Table 8-8: TACACS+ Log Messages

Component	Message	Cause
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ request needed, but no servers are configured.
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ request sent to server x.x.x.x but no response was received.
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	No key configured for the specified server.
TACACS+	TACACS+: received invalid packet type from server.	Received packet type that is not supported.
TACACS+	TACACS+: invalid major version in received packet.	Major version mismatch.
TACACS+	TACACS+: invalid minor version in received packet.	Minor version mismatch.

Table 8-9: LLDP Log Message

Component	Message	Cause
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	Unsupported LLDP packet received.

Table 8-10: SNTP Log Message

Component	Message	Cause
SNTP	SNTP: system clock synchronized on %s UTC	Indicates that SNTP has successfully synchronized the time of the box with the server.

Management

Table 8-11: SNMP Log Message

Component	Message	Cause
SNMP	EDB Callback: Unit Join: x.	A new unit has joined the stack.

Table 8-12: EmWeb Log Messages

Component	Message	Cause
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	A user attempted to connect via telnet when the maximum number of telnet sessions were already active.
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	A user attempted to connect via SSH when the maximum number of SSH sessions were already active.
EmWeb	Handle table overflow	All the available EmWeb connection handles are being used and the connection could not be made.
EmWeb	*ConnectionType* EmWeb socket accept() failed: errno	Socket accept failure for the specified connection type.
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	Socket receive failure.
EmWeb	EmWeb: connection allocation failed	Memory allocation failure for the new connection.
EmWeb	EMWEB TransmitPending : EWOULDBLOCK error sending data	Socket error on send.
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb handle index not valid.
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	The receive buffer limit has been reached. Bad request or DoS attack.
EmWeb	EmWeb accept: XXXX	Accept function for new SSH connection failed. XXXX indicates the error info.

Table 8-13: CLI_UTIL Log Messages

Component	Message	Cause
CLI_UTIL	Telnet Send Failed errno = 0x%x	Failed to send text string to the telnet client.
CLI_UTIL	osapiFsDir failed	Failed to obtain the directory information from a volume's directory.

Table 8-14: WEB Log Messages

Component	Message	Cause
WEB	Max clients exceeded	This message is shown when the maximum allowed java client connections to the switch is exceeded.
WEB	Error on send to sockfd XXXX, closing connection	Failed to send data to the java clients through the socket.
WEB	# (XXXX) Form Submission Failed. No Action Taken.	The form submission failed and no action is taken. XXXX indicates the file under consideration.
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Unknown error returned while downloading file using TFTP from web interface
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Unknown error returned while uploading file using TFTP from web interface.
WEB	Web UI Screen with unspecified access attempted to be brought up	Failed to get application-specific authorization handle provided to EmWeb/ Server by the application in ewsAuthRegister(). The specified web page will be served in read-only mode.

Table 8-15: CLI_WEB_MGR Log Messages

Component	Message	Cause
CLI_WEB_MGR	File size is greater than 2K	The banner file size is greater than 2K bytes.
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	When the number of rows exceeds the maximum allowed rows

Table 8-16: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unable to create the global (data) semaphore	Failed to create semaphore for global data protection.
SSHD	SSHD: Msg Queue is full, event = XXXX	Failed to send the message to the SSHD message queue as message queue is full. XXXX indicates the event to be sent

Table 8-16: SSHD Log Messages

Component	Message	Cause
SSHD	SSHD: Unknown UI event in message, event=XXXX	Failed to dispatch the UI event to the appropriate SSHD function as it’s an invalid event. XXXX indicates the event to be dispatched.
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	Failed to send the message to the SSHD message queue

Table 8-17: SSLT Log Messages

Component	Message	Cause
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	Exceeded maximum allowed SSLT connections.
SSLT	SSLT: Error creating Secure server socket6	Failed to create secure server socket for IPV6.
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	Failed to open connection to unsecure server. XXXX is the unsecure server socket address. YYYY is the result returned from connect function and ZZZZ is the error code.
SSLT	SSLT: Msg Queue is full, event=XXXX	Failed to send the received message to the SSLT message queue as message queue is full. XXXX indicates the event to be sent.
SSLT	SSLT: Unknown UI event in message, event=XXXX	Failed to dispatch the received UI event to the appropriate SSLT function as it’s an invalid event. XXXX indicates the event to be dispatched.
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	Failed to send the message to the SSLT message queue.
SSLT	SSLT: Error loading certificate from file XXXX	Failed while loading the SSLcertificate from specified file. XXXX indicates the file from where the certificate is being read.
SSLT	SSLT: Error loading private key from file	Failed while loading private key for SSL connection.
SSLT	SSLT: Error setting cipher list (no valid ciphers)	Failed while setting cipher list.
SSLT	SSLT: Could not delete the SSL semaphores	Failed to delete SSL semaphores during cleanup.of all resources associated with the OpenSSL Locking semaphores.

Table 8-18: User_Manager Log Messages

Component	Message	Cause
User_Manager	User Login Failed for XXXX	Failed to authenticate user login. XXXX indicates the username to be authenticated.
User_Manager	Access level for user XXXX could not be determined. Setting to READ_ONLY.	Invalid access level specified for the user. The access level is set to READ_ONLY. XXXX indicates the username.
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	Failed to migrate the config file. XXXX is the config file name. YYYY is the old version number and ZZZZ is the new version number.

Switching

Table 8-19: Protected Ports Log Messages

Component	Message	Cause
Protected Ports	Protected Port: failed to save configuration	This appears when the protected port configuration cannot be saved
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protectedPort	This appears when protectedPortCfgRWLock Fails
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when nimRegisterIntfChange with VLAN fails
Protected Ports	Cannot add intIfNum xxx to group yyy	This appears when an interface could not be added to a particular group.
Protected Ports	unable to set protected port group	This appears when a dtl call fails to add interface mask at the driver level
Protected Ports	Cannot delete intIfNum xxx from group yyy	This appears when a dtl call to delete an interface from a group fails
Protected Ports	Cannot update group YYY after deleting interface XXX	This message appears when an update group for a interface deletion fails
Protected Ports	Received an interface change callback while not ready to receive it	This appears when an interface change call back has come before the protected port component is ready.

Table 8-20: IP Subnet VLANS Log Messages

Component	Message	Cause
IPsubnet vlans	ERROR vlanIpSubnetSubnetValid :Invalid subnet	This occurs when an invalid pair of subnet and netmask has come from the CLI
IPsubnet vlans	IP Subnet Vlans: failed to save configuration	This message appears when save configuration of subnet vlans failed
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	This appears when a read/write lock creations fails
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications
IPsubnet vlans	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
IPsubnet vlans	vlanIpSubnetDtlVlanCreate: Failed	This appears when a dtl call fails to add an entry into the table
IPsubnet vlans	vlanIpSubnetSubnetDeleteApply: Failed	This appears when a dtl fails to delete an entry from the table
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	This appears when a dtl fails to add an entry for a vlan add notify event.
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 8-21: Mac-based VLANs Log Messages

Component	Message	Cause
Mac based VLANS	MAC VLANs: Failed to save configuration	This message appears when save configuration of Mac vlans failed
Mac based VLANS	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	This appears when a read/write lock creations fails
Mac based VLANS	Unable to register for VLAN change callback	This appears when this component unable to register for vlan change notifications
Mac based VLANS	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	This appears when a semaphore deletion of this component fails.
Mac based VLANS	vlanMacAddApply: Failed to add an entry	This appears when a dtl call fails to add an entry into the table
Mac based VLANS	vlanMacDeleteApply: Unable to delete an Entry	This appears when a dtl fails to delete an entry from the table
Mac based VLANS	vlanMacVlanChangeCallback: Failed to add an entry	This appears when a dtl fails to add an entry for a vlan add notify event.

Table 8-21: Mac-based VLANs Log Messages

Component	Message	Cause
Mac based VLANS	vlanMacVlanChangeCallback: Failed to delete an entry	This appears when a dtl fails to delete an entry for an vlan delete notify event.

Table 8-22: 802.1x Log Messages

Component	Message	Cause
802.1X	*function*: Failed calling dot1xIssueCmd	802.1X message queue is full
802.1X	*function:* EAP message not received from server	RADIUS server did not send required EAP message
802.1X	*function*: Out of System buffers	802.1X cannot process/transmit message due to lack of internal buffers
802.1X	*function*: could not set state to <authorized/ unauthorized>, intf xxx	DTL call failed setting authorization state of the port
802.1X	dot1xApplyConfigData: Unable to <enable/ disable> dot1x in driver	DTL call failed enabling/disabling 802.1X
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	Failed sending message to RADIUS server
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex=xxx	Failed sending accounting start to RADIUS server
802.1X	*function*: failed sending terminate cause, intf xxx	Failed sending accounting stop to RADIUS server

Table 8-23: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	*function*: osapiMessageSend failed	IGMP Snooping message queue is full
IGMP Snooping	Failed to set global igmp snooping mode to xxx	Failed to set global IGMP Snooping mode due to message queue being full
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	Failed to set interface IGMP Snooping mode due to message queue being full
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	Failed to set interface multicast router mode due to IGMP Snooping message queue being full
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	Failed to set VLAN IGM Snooping mode due to message queue being full

Table 8-23: IGMP Snooping Log Messages

Component	Message	Cause
IGMP Snooping	Failed to set igmp mrouter mode %d for interface xxx on Vlan yyy	Failed to set VLAN multicast router mode due to IGMP Snooping message queue being full
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	Could not allocate buffers for small IGMP packets
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	Could not allocate buffers for large IGMP packets

Table 8-24: GARP/GVRP/GMRP Log Messages

Component	Message	Cause
GARP/GVRP/ GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	The garpQueue is full, logs specifics of the message content like internal interface number, type of message etc.
GARP/GVRP/ GMRP	GarpSendPDU: QUEUE SEND FAILURE	The garpPduQueue is full, logs specific of the GPDU, internal interface number, vlan id, buffer handle etc.
GARP/GVRP/ GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
GARP/GVRP/ GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	Traces the build up of message queue. Helpful in determining the load on GARP.
GARP/GVRP/ GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	Mismatch between the gmd (gmrp database) and MFDB.
GARP/GVRP/ GMRP	gmd_create_entry**:** GMRP failure adding MFDB entry: vlan %d and address %s	MFDB table is full.

Table 8-25: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adReceiveMachine: received default event %x	Received a LAG PDU and the RX state machine is ignoring this LAGPDU

Table 8-25: 802.3ad Log Messages

Component	Message	Cause
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	The event sent to NIM was not completed successfully

Table 8-26: FDB Log Message

Component	Message	Cause
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	Unable to set the age time in the hardware

Table 8-27: Double VLAN Tag Log Message

Component	Message	Cause
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 8-28: IPv6 Provisioning Log Message

Component	Message	Cause
IPV6 Provisioning	ipv6ProvIntfIsConfigurable: Error accessing IPv6 Provisioning config data for interface %d	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 8-29: MFDB Log Message

Component	Message	Cause
MFDB	mfdbTreeEntryUpdate: entry does not exist	Trying to update a non existing entry

Table 8-30: 802.1Q Log Messages

Component	Message	Cause
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue is full.
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	This accommodates for reserved vlan ids. i.e. 4094 - x
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	Typically encountered during clear Vlan and clear config
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	If this vlan is a learnt via GVRP then we cannot modify it’s member set via management.

Table 8-31: 802.1S Log Messages

Component	Message	Cause
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	The message Queue is full.
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	The current conditions, like port is not enabled or we are currently not finished processing another BPDU on the same interface, does not allow us to process this BPDU
802.1S	dot1sBpduTransmit(): could not get a buffer	Out of system buffers

Table 8-32: Port Mac Locking Log Message

Component	Message	Cause
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	A default configuration does not exist for this interface. Typically a case when a new interface is created and has no pre-configuration.

Table 8-33: Protocol-based VLANs Log Messages

Component	Message	Cause
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	Appears when nimRegisterIntfChange fails to register pbVlan for link state changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with vlans	Appears when vlanRegisterForChange fails to register pbVlan for vlan changes.
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	Appears when nvStoreRegister fails to register save and restore functions for configuration save.

QoS

Table 8-34: ACL Log Messages

Component	Message	Cause
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	The combination of all ACLs applied to an interface has resulted in requiring more rules than the platform supports.
ACL	ACL *name*, rule *x*: This rule is not being logged	The ACL configuration has resulted in a requirement for more logging rules than the platform supports. The specified rule is functioning normally except for the logging action.
ACL	aclLogTask: error logging ACL rule trap for correlator *number*	The system was unable to send an SNMP trap for this ACL rule which contains a logging attribute.
ACL	IP ACL *number*: Forced truncation of one or more rules during config migration	While processing the saved configuration, the system encountered an ACL with more rules than is supported by the current version. This may happen when code is updated to a version supporting fewer rules per ACL than the previous version.

Table 8-35: CoS Log Message

Component	Message	Cause
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	The COS component was unable to apply the saved configuration and has initialized to the factory default settings.

Table 8-36: DiffServ Log Messages

Component	Message	Cause
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	While attempting to clear the running configuration an error was encountered in removing the current settings. This may lead to an inconsistent state in the system and resetting is advised.
DiffServ	Policy invalid for service intf: "policy *name*, intIfNum *x*, direction *y*	The DiffServ policy definition is not compatible with the capabilities of the interface specified. Check the platform release notes for information on configuration limitations.

Routing/IPv6 Routing

Table 8-37: DHCP Relay Log Messages

Component	Message	Cause
DHCP relay	REQUEST hops field more than config value	The DHCP relay agent has processed a DHCP request whose HOPS field is larger than the maximum value allowed. The relay agent will not forward a message with a hop count greater than 4.
DHCP relay	Request's seconds field less than the config value	The DHCP relay agent has processed a DHCP request whose SECS field is larger than the configured minimum wait time allowed.
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	The DHCP relay agent has processed an invalid DHCP packet. Such packets are discarded by the relay agent.

Table 8-38: OSPFv2 Log Messages

Component	Message	Cause
OSPFv2	Best route client deregistration failed for OSPF Redist	OSPFv2 registers with the IPv4 routing table manager (“RTO”) to be notified of best route changes. There are cases where OSPFv2 deregisters more than once, causing the second deregistration to fail. The failure is harmless.
OSPFv2	XX_Call() failure in _checkTimers for thread 0x869bcc0	An OSPFv2 timer has fired but the message queue that holds the event has filled up. This is normally a fatal error.
OSPFv2	Warning: OSPF LSDB is 90% full (22648 LSAs).	OSPFv2 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv2 logs this warning. The warning includes the current size of the database.
OSPFv2	The number of LSAs, 25165, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv2 LSDB becomes full, OSPFv2 logs this message. OSPFv2 reoriginates its router LSAs with the metric of all non-stub links set to the maximum value to encourage other routers to not compute routes through the overloaded router.
OSPFv2	Dropping the DD packet because of MTU mismatch	OSPFv2 ignored a Database Description packet whose MTU is greater than the IP MTU on the interface where the DD was received.
OSPFv2	LSA Checksum error in LsUpdate, dropping LSID 1.2.3.4 checksum 0x1234.	OSPFv2 ignored a received link state advertisement (LSA) whose checksum was incorrect.

Table 8-39: OSPFv3 Log Messages

Component	Message	Cause
OSPFv3	Best route client deregistration failed for OSPFv3 Redist	OSPFv3 registers with the IPv6 routing table manager (“RTO6”) to be notified of best route changes. There are cases where OSPFv3 deregisters more than once, causing the second deregistration to fail. The failure is harmless.

Table 8-39: OSPFv3 Log Messages

Component	Message	Cause
OSPFv3	Warning: OSPF LSDB is 90% full (15292 LSAs).	OSPFv3 limits the number of Link State Advertisements (LSAs) that can be stored in the link state database (LSDB). When the database becomes 90 or 95 percent full, OSPFv3 logs this warning. The warning includes the current size of the database.
OSPFv3	The number of LSAs, 16992, in the OSPF LSDB has exceeded the LSDB memory allocation.	When the OSPFv3 LSDB becomes full, OSPFv3 logs this message. OSPFv3 reoriginates its router LSAs with the R-bit clear indicating that OSPFv3 is overloaded.
OSPFv3	LSA Checksum error detected for LSID 1.2.3.4 checksum 0x34f5. OSPFv3 Database may be corrupted.	OSPFv3 periodically verifies the checksum of each LSA in memory. OSPFv3 logs this

Table 8-40: Routing Table Manager Log Messages

Component	Message	Cause
Routing Table Manager	RTO is full. Routing table contains 8000 best routes, 8000 total routes.	The routing table manager, also called “RTO,” stores a limited number of best routes, based on hardware capacity. When the routing table becomes full, RTO logs this alert. The count of total routes includes alternate routes, which are not installed in hardware.
Routing Table Manager	RTO no longer full. Bad adds: 10. Routing table contains 7999 best routes, 7999 total routes.	When the number of best routes drops below full capacity, RTO logs this notice. The number of bad adds may give an indication of the number of route adds that failed while RTO was full, but a full routing table is only one reason why this count is incremented.

Table 8-41: VRRP Log Messages

Component	Message	Cause
VRRP	Changing priority to 255 for virtual router with VRID 1 on interface 1/0/1	When the router is configured with the address being used as the virtual router ID, the router's priority is automatically set to the maximum value to ensure that the address owner becomes the VRRP master.
VRRP	Changing priority to 100 for virtual router with VRID 1 on interface 1/0/1	When the router is no longer the address owner, Switch CLI reverts the router's priority to the default.
VRRP	vrrpPacketValidate: Invalid TTL	VRRP ignored an incoming message whose time to live (TTL) in the IP header was not 255.

Table 8-42: ARP Log Message

Component	Message	Cause
ARP	ARP received mapping for IP address xxx to MAC address yyy. This IP address may be configured on two stations.	When we receive an ARP response with different MAC address from another station with the same IP address as ours. This might be a case of misconfiguration.

Table 8-43: RIP Log Message

Component	Message	Cause
RIP	RIP : discard response from xxx via unexpected interface	When RIP response is received with a source address not matching the incoming interface's subnet.

Table 8-44: DHCP6 Log Message

Component	Message	Cause
DHCP6	relay_to_server: Cannot relay to relay server intf xxx: not IPv6 enabled	Relay is enabled but neither the outgoing interface nor the server IP address is specified.

Multicast

Table 8-45: Cache Log Messages

Component	Message	Cause
Cache	Out of memory when creating entry.	When we run out of memory while creating a new cache (MFC) entry
Cache	Out of memory when creating cache.	When we run out of memory while creating the cache itself

Table 8-46: IGMP Log Messages

Component	Message	Cause
IGMP	Error creating IGMP pipe Error opening IGMP pipe	When we fail to create / open IGMP pipe for Mcast control messages
IGMP	Error creating IGMP data pipe Error opening IGMP data pipe	When we fail to create / open IGMP data pipe for Mcast data messages
IGMP	Error getting memory for source record	When we are unable to allocate memory for a source record in the received IGMP V3 report
IGMP	Failed getting memory for new group	When we are unable to allocate memory for a group record in the received IGMP V3/V2/V1 report

Table 8-47: IGMP-Proxy Log Messages

Component	Message	Cause
IGMP-Proxy	Error getting memory for igmp host group record	When we are unable to allocate memory for the IGMP group record in the Host (Proxy) table
IGMP-Proxy	Error getting memory for source record	When we are unable to allocate memory for the IGMP source record in the Host (Proxy) table

Table 8-48: PIM-SM Log Messages

Component	Message	Cause
PIM-SM	PIM-SM not initialized	This message arises when trying to activate pimsm interfaces or receiving pimsm packets when pimsm component is not initialized.
PIM-SM	Unable to take *xxx* semaphore	This message is logged when failed to acquire semaphore to access source list or group list or candidate Rp list or virtual interface list. The xxx specifies the list for which the access is denied.
PIM-SM	Warning : Could not send packet type xxx (pimsm packet type) on rtrIfNum	this warning is logged when failed to send a pimsm control packet on the specified router interface.
PIM-SM	add_kernel_cache : memory allocation failed	This message is logged when there is insufficient memory to add an mroute entry into cache.
PIM_SM	Config error. Trying to add static RP. Dynamic RP with same ip addr exists	Router learns RP-group mapping through Bootstrap messages received.This message pops when the static RP is configured which conflicts the mapping learnt dynamically through Bootstrap messages.
PIM-SM	Inner xxx(source/group) address of register message is invalid	This log message appears when a register message is received with invalid inner ip source or group address.

Table 8-49: PIM-DM Log Messages

Component	Message	Cause
PIM-DM	Out of memory when creating xxx	This message is logged when there is insufficient memory to accommodate a new neighbor/(S,G) Entry, Prune, Graft, Join etc.
PIM-DM	Error entry->ll_xxx LL creation error	This message is logged when the SLL creation is Failed.
PIM-DM	pim_interface_set: Could not give taskSema	This message is logged when Task synchronization Semaphore release fails.
PIM-DM	Error initializing CACHE	This message is logged when the PIM-DM (S,G) entry Cache table initialization fails.

Table 8-49: PIM-DM Log Messages

Component	Message	Cause
PIM-DM	Error creating PIM-DM pipe	This message is logged when the PIM-DM Pipe (that receives control messages) creation fails.

Table 8-50: DVMRP Log Messages

Component	Message	Cause
DVMRP	dvmrp_send_graft: failed getting memory for graft	Failed to allocate memory while sending a graft
DVMRP	dvmrp_register_neighbor: failed getting memory for nbr	Failed to allocate memory while registering a neighbor
DVMRP	dvmrp_recv_prune: failed getting memory for prune	Failed to allocate memory while receiving a prune
DVMRP	dvmrp_new_route: failed getting memory for route	Failed to get memory for a new route entry
DVMRP	dvmrp_prepare_routes: failed getting memory for dvmrp_ann_rt	Failed to get memory while announcing a new route entry

Stacking

Table 8-51: EDB Log Message

Component	Message	Cause
EDB	EDB Callback: Unit Join: <num>.	Unit <num> has joined the stack.

Technologies

Table 8-52: System General Error Messages

Component	Message	Cause
OS	Invalid USP unit = x, slot = x, port =x	A port was not able to be translated correctly during the receive.

Table 8-52: System General Error Messages

Component	Message	Cause
OS	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	Failed to add an L2 address to the MAC table. This should only happen when a hash collision occurs or the table is full.
OS	Failed installing mirror action - rest of the policy applied successfully	A previously configured probe port is not being used in the policy. The release notes state that only a single probe port can be configured
OS	Policy x does not contain rule x	The rule was not added to the policy due to a discrepancy in the rule count for this specific policy . Additionally, the message can be displayed when an old rule is being modified, but the old rule is not in the policy
OS	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x	An issue installing the policy due to a possible duplicate hash
OS	ACL x not found in internal table	Attempting to delete a non-existent ACL
OS	ACL internal table overflow	Attempting to add an ACL to a full table
OS	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	Attempting to configure the bandwidth beyond it’s capabilities
OS	USL: failed to put sync response on queue	A response to a sync request was not enqueued. This could indicate that a previous sync request was received after it was timed out
OS	USL: failed to sync ipmc table on unit=x	Either the transport failed or the message was dropped
OS	usl_task_ipmc_msg_send(): failed to send with x	Either the transport failed or the message was dropped
OS	USL: No available entries in the STG table	The Spanning Tree Group table is full in USL
OS	USL: failed to sync stg table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: A Trunk doesn't exist in USL	Attempting to modify a Trunk that doesn’t exist
OS	USL: A Trunk being created by bcmx already existed in USL	Possible synchronization issue between the application, hardware, and sync layer
OS	USL: A Trunk being destroyed doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.

Table 8-52: System General Error Messages

Component	Message	Cause
OS	USL: A Trunk being set doesn't exist in USL	Possible synchronization issue between the application, hardware, and sync layer.
OS	USL: failed to sync trunk table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: Mcast entry not found on a join	Possible synchronization issue between the application, hardware, and sync layer
OS	USL: Mcast entry not found on a leave	Possible synchronization issue between the application, hardware, and sync layer
OS	USL: failed to sync dvlan data on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: failed to sync policy table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: failed to sync VLAN table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	Invalid LAG id x	Possible synchronization issue between the BCM driver and HAPI
OS	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	Uport not valid from BCM driver.
OS	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP not able to be calculated from the learn event for BCM driver.
OS	Unable to insert route R/P	Route ‘R’ with prefix ‘P’ could not be inserted in the hardware route table. A retry will be issued.
OS	Unable to Insert host H	Host ‘H’ could not be inserted in hardware host table. A retry will be issued.
OS	USL: failed to sync L3 Intf table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: failed to sync L3 Host table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: failed to sync L3 Route table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued

Table 8-52: System General Error Messages

Component	Message	Cause
OS	USL: failed to sync initiator table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: failed to sync terminator table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued
OS	USL: failed to sync ip-multicast table on unit=x	Could not synchronize unit x due to a transport failure or API issue on remote unit. A synchronization retry will be issued

O/S Support

Table 8-53: OSAPI Log Messages

Component	Message	Cause
OSAPI	ftruncate failed – File resides on a read-only file system.	ftruncate is called to correctly set the file's size in the file system after a write. The file system is R/W so this msg indicates the file system may be corrupted.
OSAPI	ftruncate failed – File is open for reading only.	ftruncate is called to correctly set the file's size in the file system after a write. The file is opened for R/W so this msg indicates the file system may be corrupted.
OSAPI	ftruncate failed – File descriptor refers to a file on which this operation is impossible.	ftruncate is called to correctly set the file's size in the file system after a write. This msg indicates the file system may be corrupted.
OSAPI	ftruncate failed – Returned an unknown code in errno.	ftruncate is called to correctly set the file's size in the file system after a write. This msg indicates the file system may be corrupted.
OSAPI	ping: bad host!	The address requested to ping can not be converted to an Internet address.
OSAPI	osapiTaskDelete: Failed for (XX) error YYY	The requested task can not be deleted because: the requested deletion is called from an ISR, the task is already deleted, or the task ID is invalid.

Table 8-53: OSAPI Log Messages (continued)

Component	Message	Cause
OSAPI	osapiCleanupIf: NetIPGet	During the call to remove the interface from the route table, the attempt to get an ipv4 interface address from the stack failed.
OSAPI	osapiCleanupIf: NetMaskGet	During the call to remove the interface from the route table ,the attempt to get the ipv4 interface mask from the stack failed.
OSAPI	osapiCleanupIf: NetIpDel	During the call to remove the interface from the route table, the attempt to delete the primary ipv4 address from the stack failed.
OSAPI	osapiSemaTake failed	The requested semaphore can not be taken because: the call is made from an ISR or the semaphore ID is invalid.

Chapter 9
Captive Portal Commands

The Captive Portal feature is a software implementation that blocks clients from accessing the network until user verification has been established. Verification can be configured to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted.

The Authentication server supports both HTTP and HTTPS web connections. In addition, Captive Portal can be configured to use an optional HTTP port (in support of HTTP Proxy networks). If configured, this additional port is then used exclusively by Captive Portal. Note that this optional port is in addition to the standard HTTP port 80 which is currently being used for all other web traffic.

Captive Portal Global Commands

The commands in this section are related to Captive Portal Global configurations.

captive-portal

Use this command to enter the captive portal configuration mode.

Format	`captive-portal`
Mode	Global Configuration mode

enable

Use this command to globally enable captive portal.

Default	disabled
Format	`enable`
Mode	Captive Portal Configuration mode

no enable

Use this command to globally disable captive portal.

Default	disabled
Format	`no enable`
Mode	Captive Portal Configuration mode

http port

Use this command to configure an additional HTTP port for captive portal to monitor. The valid range is from 0 to 65535.

Default	80
Format	`http port  <0-65535>`
Mode	Captive Portal Configuration mode

no http port

Use this command to reset the HTTP port to the default number 80.

Format	`no http port`
Mode	Captive Portal Configuration mode

https port

Use this command to configure an additional HTTPS port for captive portal to monitor. The valid range is from 0 to 65535.

Default	443
Format	`https port  <0-65535>`
Mode	Captive Portal Configuration mode

no https port

Use this command to reset the HTTPs port to the default HTTPS port 443.

Format	`no https port`
Mode	Captive Portal Configuration mode

authentication timeout

Use this command to configure the authentication timeout. If the user does not enter valid credentials within this time limit, the authentication page needs to be served again in order for the client to gain access to the network.

Default	300
Format	`authentication timeout` *`<60-600>`*
Mode	Captive Portal Configuration mode

no authentication timeout

Use this command to reset the authentication timeout to the default.

Default	300
Format	`no authentication timeout`
Mode	Captive Portal Configuration mode

show captive-portal

Use this command to display the status of the captive portal feature.

Format	`show captive-portal`
Mode	Privileged EXEC mode

Term	Definition
Administrative Mode	The administrative mode is enabled or disabled.
Operational Status	The Operational status is enabled or disabled.
Disable Reason	If the operational status is disabled. This field shows the reason why the operational is disabled.
CP IP Address	It is the captive portal server IP address.

Example

```
(switch)#show captive-portal
Administrative Mode....................... Disabled
Operational Status........................ Disabled
Disable Reason............................ Administrator Disabled
CP IP Address................. 1.2.3.4
```

show captive-portal status

Use this command to report the status of all captive portal instances in the system.

Format	`show captive-portal status`
Mode	Privileged EXEC mode

Term	Definition
Additional HTTP Port	The additional HTTP port for captive portal to monitor. Captive portal only monitors port 80 by default.
Additional HTTP Secure Port	The additional HTTPs port for captive portal to monitor. Captive portal only monitors port 443 by default.
Peer Switch Statistics Reporting Interval	
Authentication Timeout	The timeout for the authentication page to be served again.
Supported Captive Portals	The maximum number of captive portal instances supported by switch. It supports up to 10 instances.
Configured Captive Portals	The number of created captive portal instances.

Term	Definition
Active Captive Portals	The number of active captive portal instances.
System Supported Users	The maximum number of user can be authenticated.
Local Supported Users	The maximum number of local user can be created.
Authenticated Users	The number of the authenticated users.

Example

```
(switch)#show captive-portal status
Additional HTTP Port........................... 0
Additional HTTP Secure Port.................... 0
Peer Switch Statistics Reporting Interval...... 120
Authentication Timeout......................... 300
Supported Captive Portals...................... 10
Configured Captive Portals..................... 1
Active Captive Portals......................... 0
System Supported Users......................... 1024
Local Supported Users.......................... 128
Authenticated Users............................ 0
```

Captive Portal Configuration Commands

The commands in this section are related to captive portal configurations.

configuration (Captive Portal)

Use this command to enter the captive portal instance mode. The captive portal configuration identified by CP ID 1 is the default CP configuration. The system supports a total of ten CP configurations.

Format	`configuration <`*`1-10`*`>`
Mode	Captive Portal Configuration mode

no configuration

Use this command to delete a CP configuration. The default configuration cannot be deleted.

Format	`no configuration <1-10>`
Mode	Captive Portal Configuration mode

enable (Instance)

Use this command to enable a captive portal configuration.

Default	enable
Format	`enable`
Mode	Captive Portal Instance mode

no enable

Use this command to disable a configuration.

Default	enable
Format	`no enable`
Mode	Captive Portal Instance mode

name

Use this command to configure the name for a captive portal configuration. The cp-name can be up to 32 alphanumeric characters in length.

Default	Configuration 1 has the name “Default” by default. All other configurations have no name by default.
Format	`name <cp-name>`
Mode	Captive Portal Instance mode

no name

Use this command to remove a configuration name.

Format	`no name`
Mode	Captive Portal Instance mode

protocol

Use this command to configure the protocol mode for a captive portal configuration. The default protocol is http.

Default	http
Format	`protocol { http | https }`
Mode	Captive Portal Instance mode

verification

Use this command to configure the verification mode for a captive portal configuration. User verification can be configured to allow access for guest users; users that do not have assigned user names and passwords. User verification can also be configured to allow access for authenticated users. Authenticated users are required to enter a valid user name and password that must first be validated against the local database or a RADIUS server. Network access is granted once user verification has been confirmed.

Default	guest
Format	`verification { guest | local | radius }`
Mode	Captive Portal Instance mode

group

Use this command to configure a group ID for this captive portal configuration. If a group number is configured, the user entry (Local or RADIUS) must be configured with the same name and the group to authenticate to this captive portal instance. The group ID must be xist first. You can use the command “user group <1-10>” to create a group ID. The default group ID is 1 for a captive portal configuration.

Default	1
Format	`group <1-10>`
Mode	Captive Portal Instance mode

no group

Use this command to reset the group number to the default.

Default	1
Format	`no group <1-10>`
Mode	Captive Portal Instance mode

redirect (Captive Portal)

Use this command to enable the redirect mode for a captive portal configuration. Use the “no” form of this command to disable redirect mode.

Default	disable
Format	`redirect`
Mode	Captive Portal Instance mode

no redirect

Use this command to disable redirect mode.

Format	`no redirect`
Mode	Captive Portal Instance mode

redirect-url

Use this command to configure the redirect URL for a captive portal configuration. The url is the URL for redirection which can be up to 512 characters in length.

Format	`redirect-url` *`url`*
Mode	Captive Portal Instance mode

max-bandwidth-down

Use this command configures the maximum rate at which a client can receive data from the network. The rate is in bits per seconds. 0 indicates limit not enforced.

Default	0
Format	`max-bandwidth-down` *`<0-536870911>`*
Mode	Captive Portal Instance mode

no max-bandwidth-down

Use this command to reset the maximum rate to the default.

Format	`no max-bandwidth-down`
Mode	Captive Portal Instance mode

max-bandwidth-up

Use this command to configure the maximum rate at which a client can send data into the network. The rate is in bits per seconds. 0 indicates limit not enforced.

Default	0
Format	`max-bandwidth-up <0-536870911>`
Mode	Captive Portal Instance mode

no max-bandwidth-up

Use this command to reset the maximum rate to the default**.**

Format	`no max-bandwidth-up`
Mode	Captive Portal Instance mode

max-input-octets

Use this command to configure the maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. The number of octets is in bytes. 0 indicates limit not enforced.

Default	0
Format	`max-input-octets  <0-4294967295>`
Mode	Captive Portal Instance mode

no max-input-octets

Use this command to reset the limit to the default.

Format	`no max-input-octets`
Mode	Captive Portal Instance mode

max-output-octets

Use this command to configure the maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. The number of octets is in bytes. 0 indicates limit not enforced Use the "no".

Default	0
Format	`max-output-octets <0-4294967295>`
Mode	Captive Portal Instance mode

no max-output-octets

Use this command to reset the limit to the default.

Format	`no max-output-octets`
Mode	Captive Portal Instance mode

max-total-octets

Use this command to configure the maximum number of octets the user is allowed to transfer, i.e., the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. The number of total octets is in bytes. 0 indicates limit not enforced. Use the "no" form of this command to reset the limit to the default.

Default	0
Format	`max-total-octets <0-4294967295>`
Mode	Captive Portal Instance mode

no max-total-octets

Use this command to reset the limit to the default.

Default	0

Format	`max-total-octets <0-4294967295>`
Mode	Captive Portal Instance mode

session-timeout (Captive Portal)

Use this command to configure the session timeout for a captive portal configuration. After this limit has been reached, the user will be disconnected. Timeout is time in seconds. 0 indicates timeout not enforced.

Default	0
Format	`session-timeout <0-86400>`
Mode	Captive Portal Instance mode

no session-timeout

Use this command to reset the session timeout to the default.

Format	`session-timeout <0-86400>`
Mode	Captive Portal Instance mode

idle-timeout

Use this command to configure the idle timeout for a captive portal configuration. 0 indicates timeout not enforced. After an idle session has been reached this, the user will be disconnected**.**

Default	0
Format	`idle-timeout <0-900>`
Mode	Captive Portal Instance mode

no idle-timeout

Use this command to reset the idle timeout to the default.

Format	`no idle-timeout`
Mode	Captive Portal Instance mode

locale

This command is not intended to be a user command. The administrator must use the WEB UI to create and customize captive portal web content. This command is primarily used by the show running-config command and process as it provides the ability to save and restore configurations using a text based format.

Default	`1`
Format	`locale <1-5>`
Mode	Captive Portal Instance mode

no locale

This command is intended to delete a locale. The default locale cannot be deleted.

Format	`no locale <1-5>`
Mode	Captive Portal Instance mode

interface (Captive Portal)

Use this command to associate an interface with a captive portal configuration.

Format	`interface` *`<unit/slot/port>`*
Mode	Captive Portal Instance Config mode

no interface

Use this command to remove an association with a captive portal configuration.

Format	`no interface <unit/slot/port>`
Mode	Captive Portal Instance Config mode

block

Use this command to block all traffic for a captive portal configuration. The administrator can block access to a captive portal configuration. When an instance is blocked no client traffic is allowed through any interfaces associated with that captive portal configuration. Blocking a captive portal instance is a temporary command executed by the administrator and not saved in the configuration.

Default	no block
Format	`block`
Mode	Captive Portal Instance mode

no block

Use this command to unblock traffic.

Format	`no block`
Mode	Captive Portal Instance mode

Captive Portal Status Commands

This section describes commands that return captive portal status.

show captive-portal configuration

Use this command to display the operational status of each captive portal configuration.

Format	`show captive-portal configuration <1-10>`
Mode	Privileged EXEC mode

Term	Definition
CP ID	The captive portal ID
CP Name	The captive portal instance name
Operational Status	The operational status is enabled or disabled.
Disable Reason	If the operational status is disabled, this field shows the reason.
Blocked Status	Blocked status shows if this captive portal instance block all traffic.
Authenticated Users	The authenticated users by this captive portal instance.

Example

```
(switch)#show captive-portal configuration 1
CP ID.................................... 1
CP Name.................................. cp1
Operational Status....................... Disabled
Disable Reason........................... Administrator Disabled
Blocked Status........................... Not Blocked
Authenticated Users...................... 0
```

show captive-portal configuration interface

Use this command to display information about all interfaces assigned to a captive portal configuration or about a specific interface assigned to a captive portal configuration. The <*1-10*> is the captive portal ID. If you do not specify an interface number, all the interfaces assigned to the captive portal configuration will be displayed.

Format	`show captive-portal configuration <1-10> interface` **[** `<unit/slot/port>` **]**
Mode	Privileged EXEC mode

Term	Definition
CP ID	The captive portal ID.
CP Name	The captive portal name.
Interface	The interface associated with the CP ID
Interface Description	The interface description
Operational Status	The operational status is enabled or disabled.
Disable Reason	The reason if the operational status is disabled.
Block Status	It shows this captive portal instance block all traffic or not.

If the interface is specified. The following term will be displayed.

Term	Definition
Authenticated users	The number of authenticated users associated with the CP ID.

Example

```
(Switch)#show captive-portal configuration 1 interface
CP ID..................................... 1
CP Name................................... cp1
                                         Operational          Block
Interface    Interface Description       Status               Status
---------   ---------------------     ----------------    ----------1/0/1
Unit:1Slot:0Port:1           Disabled           Blocked

(Switch)#show captive-portal configuration 1 interface 1/0/1
CP ID..................................... 1
CP Name................................... cp1
Interface................................. 1/0/1
Interface Description..................... Unit: 1 Slot: 0 Port: 1 Gigab
Operational Status........................ Disabled
Disable Reason............................ Interface Not Attached
Block Status.............................. Not Blocked
Authenticated Users....................... 0
```

show captive-portal configuration status

Use this command to display information about all configured captive portal configurations or about a specific captive portal configuration. The <*1-10*> is captive portal ID. If <1-10> is not entered, all the configurations are displayed.

Format	`show captive-portal configuration [ <1-10> ] status`
Mode	Privileged EXEC mode

Term	Definition
CP ID	The captive portal instance ID
CP Name	The captive portal instance name
Mode	The operational mode is enabled or disabled.
Protocol Mode	The protocol mode is https or http.
Verification Mode	The user verification mode has three modes: guest, local and radius. The default is guest mode.

If the interface is specified, the following terms are displayed.

Term	Definition
Group Name	The name of the group associated with this captive portal instance.
Redirect URL Mode	The redirect mode for this captive portal instance
Redirect URL	The redirect URL is up to 512 characters.
Session Timeout	Logout once session timeout is reached (seconds).
Idle Timeout	Logout once idle timeout is reached (seconds).
Max Bandwidth Up	Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network.
Max Bandwidth Down	Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network.
Max Input Octets	Maximum number of octets the user is allowed to transmit.After this limit has been reached the user will be disconnected.
Max Output Octets	Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected.
Max Total Octets	Maximum number of octets the user is allowed to transfer (sum of octets transmitted and received). After this limit has been reached the user will be disconnected.

Example

```
(switch)#show captive-portal configuration status
CP ID     CP Name        Mode     Protocol    Verification
-----    ----------    --------   --------    ------------
1          cp1          Enable     https       Guest
2          cp2          Enable     http        Local
3          cp3          Disable    https       Guest
(switch)#show captive-portal configuration 1 status
CP ID.......................................... 1
CP Name........................................ cp1
Mode........................................... Enabled
Protocol Mode.................................. https
Verification Mode.............................. Guest
Group Name..................................... group123
Redirect URL Mode.............................. Enabled
Redirect URL................................... www.cnn.com
Session Timeout (seconds)...................... 86400
Idle Timeout (seconds)......................... 600
Max Bandwidth Up (bytes/sec)................... 0
Max Bandwidth Down (bytes/sec)................. 0
Max Input Octets (bytes)....................... 0
Max Output Octets (bytes)...................... 0
Max Total Octets (bytes)....................... 0
```

show captive-portal configuration locales

Use this command to display locales associated with a specific captive portal configuration. *<1-10>* is captive port ID.

Format	`show captive-portal configuration <1-10> locales`
Mode	Privileged EXEC mode

Example

```
(switch)#show captive-portal configuration 1 locales
Locale Code
---------------
En
```

show captive-portal trapflags

Use this command to display which captive portal traps are enabled.

Format	`show captive-portal trapflags`
Mode	Privileged EXEC mode

Example

```
(switch)#show captive-portal trapflags
Client Authentication Failure Traps............ Disable
Client Connection Traps........................ Disable
Client Database Full Traps..................... Disable
Client Disconnection Traps..................... Disable
```

Captive Portal Client Connection Commands

This section describes captive portal client connection commands.

show captive-portal client status

Use this command to display client connection details or a connection summary for connected captive portal users. *macaddr* is Client MAC address. If no macaddr is entered, all the client status will be displayed.

Format	`show captive-portal client [ macaddr ] status`
Mode	Privileged EXEC mode

Term	Definition
Client MAC Address	The MAC address of the authenticated user
Client IP Address	The IP address of the authenticated user
Protocol	The protocol the user is using to access the network.
Verification	The verification mode for this client.
Session Time	The current session time since the client is authenticated.

If the macaddr is specified, the following terms are displayed.

Term	Definition
CP ID	The captive portal ID associated with the client
CP Name	The captive portal name associated with the client
Interface	The interface on which the client authenticated.
Interface Description	The interface description
User Name	The name of the client who is authenticated.

Example

```
(switch)#show captive-portal client status
Client MAC Address  Client IP Address  Protocol  Verification  Session
                                                                Time
-----------------   ----------------   --------  ------------   -----
0002.BC00.1290       10.254.96.47       https     Local     0d:00:01:20
0002.BC00.1291       10.254.96.48       https     Local     0d:00:05:20
0002.BC00.1292       10.254.96.49       https     Radius    0d:00:00:20

(switch)#show captive-portal client 0002.BC00.1290 status
Client MAC Address........................ 0002.BC00.1290
Client IP Address......................... 10.254.96.47
Protocol Mode............................. https
Verification Mode......................... Local
CP ID..................................... 1
CP Name................................... cp1
Interface................................. 1/0/1
Interface Description.................... Unit: 1 Slot: 0 Port: 1 Gigabit - Level
User Name................................. user123
Session Time.............................. 0d:00:00:13
```

show captive-portal client statistics

Use this command to display the statistics for a specific captive portal client. *The macaddr* is client MAC address.

Format	`show captive-portal client macaddr statistics`
Mode	Privileged EXEC mode

Term	Definition
Client MAC address	The MAC address of the authenticated client
Bytes Received	The number of bytes received from the client
Bytes Transmitted	The number of bytes transmitted to the client
Packets Received	The number of packets received from the client
Packets Transmitted	The number of packets transmitted from the client

Example

```
(switch)#show captive-portal client 0102.0304.0506 statistics
Client MAC Address........................ 0002.bc00.1290
Bytes Received............................ 0
Bytes Transmitted......................... 0
Packets Received.......................... 0
Packets Transmitted....................... 0
```

show captive-portal interface client status

Use this command to display information about clients authenticated on all interfaces or a specific interface

Format	**show captive-portal interface [**<unit/slot/port>] **client status**
Mode	Privileged EXEC mode

Term	Definition
Client Intf	Interface on which the clients are authenticated.
Client Intf Description	The interface description
MAC Address	The MAC address of the authenticated user.
IP Address	The IP address of the authenticated user.

If the interface is specified, the following terms are displayed.

Term	Definition
CP ID	The ID of the captive portal associated with the client
CP Name	The name of the captive portal associated with the client
Protocol	The protocol the client is using

Term	Definition
Verification	The user verification mode

Example

```
(switch)#show captive-portal interface client status
Client        Client
Intf       Intf Description                      MAC Address         IP Address
------      ----------------------------------     -----------------          -
--------------
1/0/1     Unit: 1 Slot: 0 Port: 1 Gigabit     0002.BC00.1290      10.254.96.47
1/0/2     Unit: 1 Slot: 0 Port: 2 Gigabit     0002.BC00.1292      10.254.96.49
1/0/3     Unit: 1 Slot: 0 Port: 3 Gigabit     0002.BC00.1293      10.254.96.50

(switch)#show captive-portal interface 1/0/1 client status
Interface................................. 1/0/1
Interface Description..................... Unit: 1 Slot: 0 Port: 1 Gigabit
Client Client
MAC Address        IP Address     CP ID     CP Name     Protocol     Verification
-----------------         ---------------    -----      --------------    ------
--        ------------
0002.BC00.1290   10.254.96.47   1            cp1            http          local
0002.BC00.1291   10.254.96.48   2            cp2            http          local
```

show captive-portal configuration client status

Use this command to display the clients authenticated to all captive portal configurations or a to specific configuration. <*1-10*> is the captive portal ID.

Format	`show captive-portal configuration [ <1-10> ] client status`
Mode	Privileged EXEC mode

Term	Definition
CP ID	The captive portal ID
CP Name	The captive portal name
Client MAC Address	The MAC address of the client associated with the captive portal instance.
Client IP Address	The IP address of the client associated with the captive portal instance
Interface	The interface on which the client is authenticated.

If the CP ID is specified, the following terms are displayed.

Term	Definition
Interface Description	The description of the interface

Example

```
(switch)#show captive-portal configuration client status
CP ID  CP Name  Client MAC Address    Client IP Address   Interface
-----  -------  ------------------    -----------------  ---------
1        cp1     0002.BC00.1290       10.254.96.47        1/0/1
2        cp2     0002.BC00.1292       10.254.96.49        1/0/3
3        cp3     0002.BC00.1293       10.254.96.50        1/0/4

(switch)#show captive-portal configuration 1 client status
CP ID.................................... 1
CP Name.................................. cp1
Client            Client
MAC Address      IP Address     Interface    Interface Description
--------------   -------------  ---------    ----------------------
0002.BC00.1290   10.254.96.47    1/0/1   Unit:1 Slot:0 Port:1 Gigabit
0002.BC00.1291   10.254.96.48    1/0/2   Unit:1 Slot:0 Port:2 Gigabit
```

captive-portal client deauthenticate

Use this command to deauthenticate a specific captive portal client. The *macaddr* is the Client MAC address.

Format	`captive-portal client deauthenticate macaddr`
Mode	Privileged EXEC mode

Captive Portal Interface Commands

The following section describes captive portal interface commands.

show captive-portal interface configuration status

Use this command to display the interface to configuration assignments for all captive portal configurations or for a specific configuration. *<1-10>* is the captive portal ID.

Format	`show captive-portal interface configuration [ <1-10>] status`
Mode	Privileged EXEC mode

Term	Definition
CP ID	The captive portal ID
CP Name	The captive portal name
Interface	The interface associated with the CP ID.
Interface Description	The description of the interface
Type	The type of the interface

Example

```
(switch)#show captive-portal interface configuration status
CP ID    CP Name    Interface    Interface Description                    Type
----- ------------  --------- ----------------------------              --------
1           Default       1/0/1        Unit: 1 Slot: 0 Port: 1 Gigabit    Physical


(switch)#show captive-portal interface configuration 1 status
CP ID..................................... 1
CP Name................................... cp1
Interface      Interface Description                Type
---------      --------------------------------- --------
1/0/1          Unit: 1 Slot: 0 Port: 1 Gigabit    Physical
```

Captive Portal Local User Commands

The following section describes captive portal local user commands.

user password

Use this command to create a local user or change the password for an existing user. The *user-id* is user ID in the range of 1-128. The *password* is the user password in the range of 8-64 characters. You can also enter encrypted password using the parameter *encrypted.*

Format	`user user-id password { password | encrypted enc-password }`
Mode	Captive Portal Configuration mode

no user

Use this command to delete a user from the local user database. If the user has an existing session, it is disconnected.

Format	`no user user-id <1-128>`
Mode	Captive Portal Configuration mode

user name

Use this command to modify the user name for a local captive portal user. *<1-128>* is the user ID and the *name* is the user name in the range of 1-32 characters. The local user must be exist before execute this command. You can create the local user using *user password* first.

Format	`user <1-128> name name`
Mode	Captive Portal Configuration mode

user group

Use this command to associate a group with a captive portal user. A user must be associated with at least one group so the last group cannot be dis-associated. <1-128> is the user ID and <1-10> is the group ID.

Default	1
Format	`user <1-128> group <1-10>`
Mode	Captive Portal Configuration mode

no user group

Use this command to dis-associate a group and user.

Format	`no user <1-128> group <1-10>`
Mode	Captive Portal Configuration mode

user session-timeout

Use this command to set the session timeout value for a captive portal user. Use the “no” form of this command to reset the session timeout to the default. The range of session timeout is 0-86400. 0 indicates use global configuration.

t

Default	0
Format	`user <1-128> session-timeout timeout`
Mode	Captive Portal Configuration mode

no user session-timeout

Use this command to reset the session timeout to the default.

Format	`no user <1-128> session-timeout`
Mode	Captive Portal Configuration mode

user idle-timeout

Use this command to set the session idle timeout value for a captive portal user. <1-128> is the user ID. The range of idle timeout is 0-900 seconds. 0 indicates use global configuration.

Default	0
Format	`user <1-128> idle-timeout timeout`
Mode	Captive Portal Configuration mode

no user idle-timeout

Use this command to reset the idle timeout to the default value.

Format	`no user <1-128> idle-timeout timeout`
Mode	Captive Portal Configuration mode

user max-bandwidth-down

Use this command to configure the bandwidth at which the client can receive data from the network. <1-128> is the user ID. The range of *bps* is <0-536870911> bps. 0 indicates use global configuration.

Default	0
Format	`user <1-128> max-bandwidth-down bps`
Mode	Captive Portal Configuration mode

no user max-bandwidth-down

Use this command to reset the limit to the default.

Format	`no user <1-128> max-bandwidth-down`
Mode	Captive Portal Configuration mode

user max-bandwidth-up

Use this command to configure the bandwidth at which the client can send data into the Network. <1-128> is the user ID. The range of *bps* is <0-536870911> bps. 0 indicates use global configuration.

Default	0
Format	`user <1-128> max-bandwidth-up bps`
Mode	Captive Portal Configuration mode

no user max-bandwidth-up

Use this command to reset the limit to the default.

Format	`no user <1-128> max-bandwidth-up`
Mode	Captive Portal Configuration mode

user max-input-octets

Use this command to limit the number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. <*1-128*> is the user ID. The range of *octets* is 0-4294967295. 0 indicates to use the global limit.

Default	0
Format	`user <1-128> max-input-octets octets`
Mode	Captive Portal Configuration mode

no user max-input-octets

Use this command to reset the limit to the default.

Format	`no user <1-128> max-input-octets`
Mode	Captive Portal Configuration mode

user max-output-octets

Use this command to limit the number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. The <*1-128*> is the user ID. The range of the *octets* is 0 – 4294967295. 0 indicates to use the global limit.

Default	0
Format	`user <1-128> max-output-octets octets`
Mode	Captive Portal Configuration mode

no user max-output-octets

Use this command to reset the limit to the default.

Default	0
Format	`no user <1-128> max-output-octets`
Mode	Captive Portal Configuration mode

user max-total-octets

Use this command to limit the number of bytes the user is allowed to transmit and receive. The maximum number of octets is the sum of octets transmitted and received. After this limit has been reached the user will be disconnected. <1-128> is the user ID. The range of *octets* is 0-4294967295. 0 indicates to use the global limit.Use the “no” form of this command to reset the limit to the default.

Default	0
Format	`user <1-128> max-total-octets` *`octets`*
Mode	Captive Portal Configuration mode

no user max-total-octets

Use this command to reset the limit to the default.

Format	`no user <1-128> max-total-octets`
Mode	Captive Portal Configuration mode

show captive-portal user

Use this command to display all configured users or a specific user in the captive portal local user database.

Format	`show captive-portal user` **[** *<1-128>* **]**
Mode	Privileged EXEC mode

Term	**Definition**
User ID	The user ID
User Name	The user name
Session Timeout	Logout once session timeout is reached (seconds). If the value is 0 then use the value configured for the captive portal.
Idle Timeout	Logout once idle timeout is reached (seconds). If the attribute is 0 then use the value configured for the captive portal.
Group ID	The group ID associated with the user
Group Name	The group name

If the user ID is specified, the following terms are displayed.

Term	**Definition**
Password Configured	If the password is configured.
Max Bandwidth Up (bytes/sec)	Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network. If the value is 0 then use the value configured for the captive portal.
Max Bandwidth Down (bytes/sec)	Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network. If the value is 0 or then use the value configured for the captive portal.
Max Input Octets (bytes)	Maximum number of octets the user is allowed to transmit.After this limit has been reached the user will be disconnected. If the value is 0 then use the value configured for the captive portal.
Max Output Octets (bytes)	Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. If the attribute is 0 then use the value configured for the captive portal.
Max Total Octets (bytes)	Maximum number of octets the user is allowed to transfer (sum of octets transmitted and received). After this limit has been reached the user will be disconnected. If the value is 0 then use the value configured for the captive portal.

Example

```
(switch)#show captive-portal user
```

```
                           Session      Idle
User ID   User Name         Timeout     Timeout        Group ID         Group Name
-------   --------------   --------     --------      --------         -----------
1         user123              10          13            1                Default
2         user234                0           0             1              Default

(switch)#show captive-portal user 1

User ID......................................... 1
User Name....................................... user123
Password Configured............................. Yes
Session Timeout................................. 0
Idle Timeout.................................... 0
Max Bandwidth Up (bytes/sec).................... 0
Max Bandwidth Down (bytes/sec).................. 0
Max Input Octets (bytes)........................ 0
Max Output Octets (bytes)....................... 0
Max Total Octets (bytes)........................ 0
Group ID             Group Name
-------- --------------------------------
1                             Default
2                             group2
```

clear captive-portal users

Use this command to delete all captive portal user entries.

Format	`clear captive-portal users`
Mode	Privileged EXEC mode

Captive Portal User Group Commands

The following section describes captive portal user group commands.

user group (Create)

Use this command to create a user group. User group 1 is created by default and cannot be deleted.

Default	1
Format	`user group <1-10>`
Mode	Captive Portal Configuration mode

no user group

Use this command to delete a user group. The default user group (1) cannot be deleted.

Format	`user group <`*`1-10`*`>`
Mode	Captive Portal Configuration mode

user group name

Use this command to configure a group name. <1-10> is the user group ID. The name can be a string up to 32 characters.

Format	`user group <1-10>  name name`
Mode	Captive Portal Configuration mode

user group rename

Use this command to change a group's ID to a different group ID.

Format	`user group `*`group-id`*`  rename  `*`new-group-id`*
Mode	Captive Portal Configuration mode

Chapter 10
Command List